Integra32™

Integrated Alarm Monitoring and Access Control

USER MANUAL

Copyright Notice

Copyright© 1995 – 2010 by RBH Access Technologies Inc.

All rights reserved Worldwide. Printed in Canada. This publication has been provided pursuant to an agreement containing restrictions on its use. No part of this book may be copied or distributed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, manual, or otherwise, or disclosed to third parties without the express written consent of RBH Access Technologies Inc., Brampton, Ontario, Canada.

Trademark

Integra32™ is the trademark of RBH Access Technologies Inc. Windows is a trademark of Microsoft Corporation. All other product names mentioned herein are the property of their respective owners. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Disclaimer

This book is provided *as is*, without warranty of any kind, either express or implied, including but not limited to performance, merchantability, or fitness for any particular purpose. Neither RBH Access Technologies Inc., nor its dealers or distributors shall be liable to any person or entity with respect to any liability, loss, or damage, caused, or alleged to have been caused directly or indirectly by this information. Further RBH Access Technologies Inc. reserves the right to revise this publication, and to make changes to the content hereof from time to time, without the obligation of RBH Access Technologies Inc. to notify any person or organization of such revision or changes.

RBH ACCESS TECHNOLOGIES INC.

2 Automatic Road, Suite 108
Brampton, Ontario
CANADA
L6S 6K8

Printing Date May 25, 2010

Integra32 Revision 4.2

Table of Contents

INTRODUCING INTEGRA32™ **2**
INTEGRA32 SERVER CLIENT NETWORK SETUP 2
GETTING TO KNOW INTEGRA32™ **3**
COMMAND BAR 3
Menu Options *4*
Toolbar Buttons *8*
DATABASE SCREEN 9
DEVICE STATUS SCREEN 10
ALARMS SCREEN 10
EVENT LOG SCREEN 11
COMMAND SCREEN **12**
DEVICE STATUS 12
HOW TO EXECUTE A COMMAND 13
Command Type *13*
ACCESS POINTS COMMANDS 14
Commands *14*
INPUT POINTS COMMANDS 16
Commands *16*
OUTPUT POINTS COMMANDS 17
Commands *17*
PANELS COMMANDS 18
Commands IRC2000 & URC2000 ..... *19*
Commands PC100 (Summit or Risco Group) *20*
Commands PC100 (Bosch) *20*
AREA AND CARDHOLDER COMMANDS 21
Commands *21*
VISITORS 22
FLOORS 22
KEYPAD COMMANDS 23
Commands *23*
ALARMS SCREEN **24**
ACKNOWLEDGE/UNACKNOWLEDGE/CLEAR 24
ALARM DETAILS 24
PROGRAMMING **27**
INTEGRA32 DATABASE 27
Users *27*
Holidays *30*
Schedules *31*
Areas *33*
Messages *34*
Networks *35*
Panels *41*
Access Points *59*
Inputs *70*
Outputs *75*
Elevators *79*
Floor Groups *81*
Access Levels *82*
CARDHOLDERS **84**
FIELDS AND OPTIONS 85
Multi Cards *86*

F Print *88*
Receipt *89*
CARDHOLDERS' TABS 90
Cards *90*
Profile Tab *93*
Photo Tab *94*
Notes Tab *95*
More Fields Tab *96*
VISITOR MANAGER 97
GENERAL 100
USER FIELDS 101
ASSETS 102
TRACK 103
PHOTO 104
REPORTS 105
HISTORY REPORTS 105
File *106*
Reports *106*
Preview *106*
DVR *109*
DATABASE REPORTS 110
Options *110*
VISITOR REPORTS 112
OPTIONS 113
SYSTEM OPTIONS 113
General *113*
Badge *115*
Font *117*
SYSTEM MESSAGES 118
ACCESS POINT ACTIVITY 119
More/Less *119*
Hide *119*
VM CONFIGURATION 120
eMail Configuration *120*
User Fields *121*
LINKS 122
GLOBAL LINKS 122
TOOLS 123
BACKUP 123
Run Backup Now *123*
Configure Auto-Backup *124*
RESTORE 125
VOID CARDS 126
FINGER PRINT 127
QUERY FINGER PRINT READER 129
BADGE TEMPLATE DESIGNER 130
CARD CUSTOM FIELDS 132
CARD IMPORT 133
Configure Import Utility *133*
Complete the configuration. *139*
Run Import Utility *142*
View Log File *143*
PROGRAM GROUPS 144
INTEGRA32™ SECURITY SYSTEM 144

Integra32™ Data Restore *145*
Integra32™ Database Maintenance *145*
Integra32™ Firmware Upgrade *145*
Integra32™ Security System *147*
Integra32™ Site Configuration *148*
Integra32™ Registration *148*
GLOSSARY **150**
LICENSE & WARRANTY **151**
INDEX **152**
READER COMMENTS **155**

About This Guide

This guide documents how to install and use the Integra32™ Security Management System as developed by RBH Access Technologies Inc. The **Integra32™** system represents the latest in access control technology specifically designed for the smaller application. Its intuitive graphical interface allows users to take advantage of the power of the **Integra32™** with a minimal amount of training.

Read this guide if you are:

- An operator who monitors security and access using Integra32™.
- A system administrator who updates Integra32™'s database.
- The system technician that installs and configures the Integra32™ onsite.

Before reading this guide

This guide assumes that you:

- Are familiar and comfortable with a personal computer.
- Know how to use a mouse.
- Are familiar with the Windows operating environment.

Conventions in this guide

Menu options, window titles, fields, and buttons are indicated by *italic typeface*. For example, "choose *Access Point Activity* from the *Option* menu" or "click *Cancel* to cancel your changes".

Keyboard actions and function keys are denoted by **bold typeface**. For example, "press **F1** to display online help".

Keyboard control sequences (i.e., using two or more keyboard keys in combination), are denoted by keys in **bold typeface** separated by a plus sign (+). For example, "press **Ctrl + Alt + Delete** to reboot the system".

Cross-references are displayed in blue, and will jump you to the associated or mentioned part of the manual. Click on the *cross-reference* when the curser changes to move to that place in the manual.

Chapter 1
Introducing Integra32™

The Integra32™ system integrates Access Control, Photo-Badging, Digital Video Recording and Alarm Monitoring into an elegant building management and security system specifically designed for the smaller application

Integra32™'s 32-bit software architecture together with a Microsoft Windows™ operating system ensures that security management needs are met easily and economically with a minimal amount of training.

The IRC-2000 Intelligent Field Panels utilize flash firmware for easy upgrades. This panel uses fully distributed intelligence for off-line operations. In addition to supporting two card readers, each IRC-2000 Intelligent Field Panel also has eight fully supervised alarm inputs along with eight outputs. The IRC2000's memory has been increased to now hold 5,000 card and can be further extended to hold 8,000 cards.

An alternate panel the URC2000 can be used along with or instead of the original IRC2000. This panel also uses fully distributed intelligence for off-line operations. In addition to supporting two card readers, each URC-2000 panel has four fully supervised alarm inputs and four outputs as well as a 3,000 card acpacity. Communication is handle through an RS485 port.

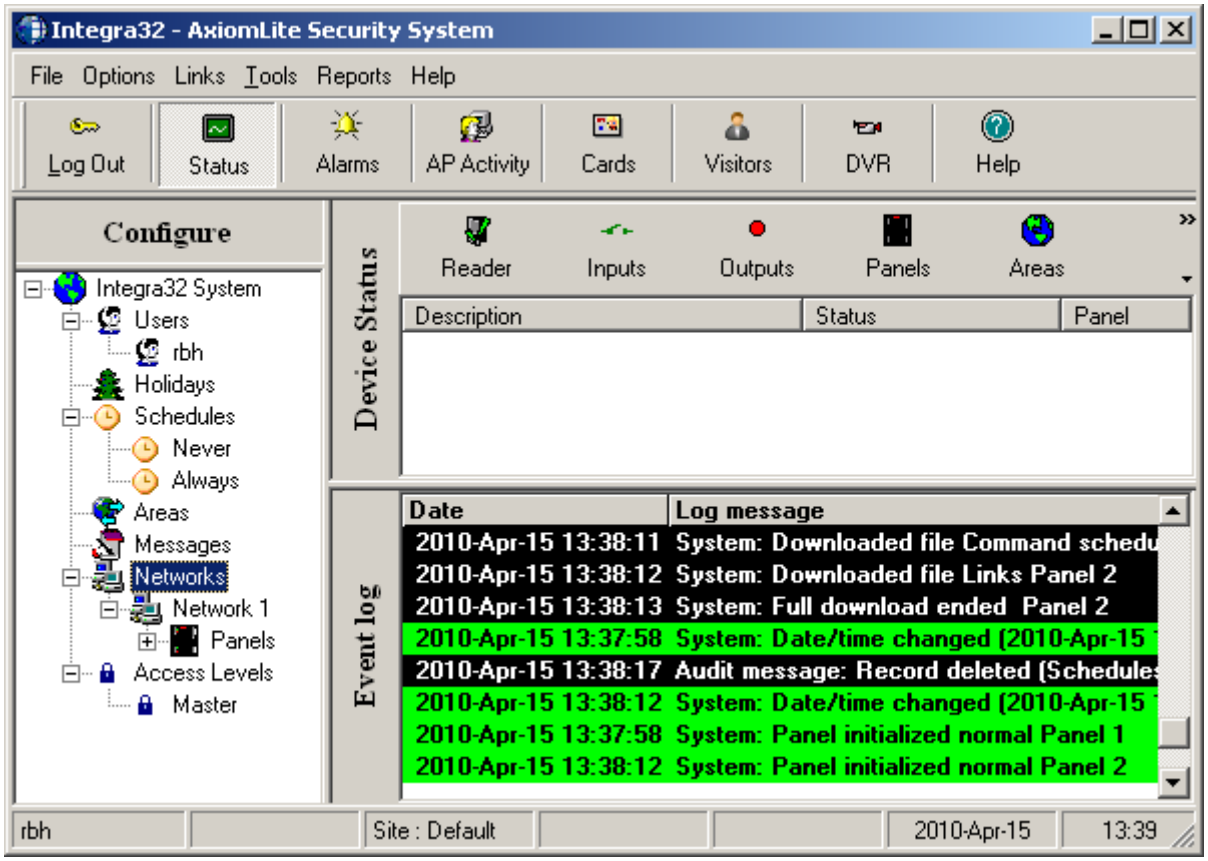
Integra32 Server Client Network Setup

Please see technical document TB63 for a step-by-step guide to installing Integra32™.

In order for a remote client to connect to the server, the server must first be running. This should not be a problem since the Integra32 server now runs as a service and should be running at all times.

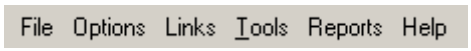
Chapter 2
Getting to Know Integra32™

Integra32™ lets you manage and monitor all your security access needs using a standard PC. There are four separate parts to the Integra32's™ main screen:



Command Bar

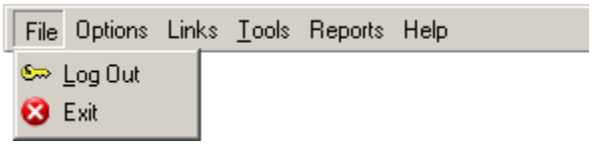
Menus and buttons to access other features of the system are available on the *Command Bar*. Integra32™ has the following menu options:



Each of these items has a drop down menu with further options that "launch" the functions contained in the drop down menu (*e.g., Log Out of the Integra32™ system*). In addition, Integra32™ provides Toolbar buttons as an optional means of launching either the same function contained in drop down menu or to launch new windows (*e.g. Cardholder window*).

Menu Options

File



Use this menu to log in/log out or to exit the Integra32™ application.

Log In & Out (Ctrl+L)

An operator must be logged in to operate the system. This ensures that all actions performed on the PC can be attributed to a particular operator.

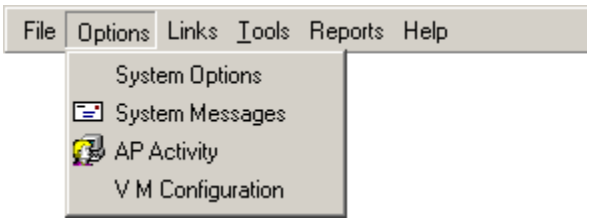
To log in, enter your full login Name and password. The default login name is "rbh" and default password is "password". Both 'Login Name' and 'Password' are not case sensitive.

An operator should log out when leaving the computer unattended or when finished his/her shift. Logging out protects the system against unauthorized access.

Exit

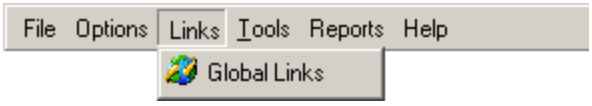
Exit will shutdown the Integra32™ System Client software.

Options



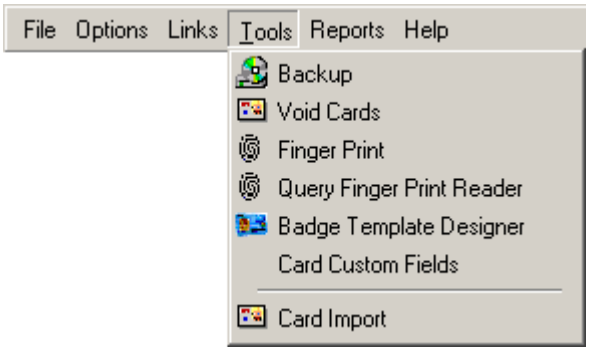
Use this menu option to customize user preferences (*through* System Options) or customize the System Messages that are displayed on the Status Screen and in the History Reports. The Access Point Activity window is also enabled here. Details of the Access Point Activity window option will be discussed in Chapter 8. Visitor Management configuration is accessed by selecting VM Configuration[1].

Links



This is where Global Links are setup; details of this are shown in Chapter 9.

Tools



The *Tools* menu gives the options for Backup, Void Cards, Finger Print[2], Query Finger Print Reader[4], Badge Template Designer[3], Card Custom Fields, and Card Import[4], which are covered in more detail in Chapter 10.

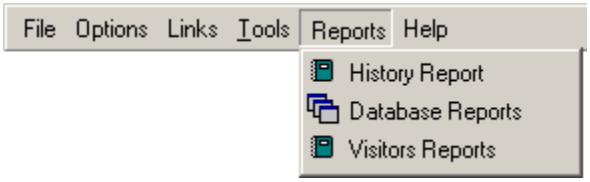
[1] This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

[2] This selection is only available if the optional license for the Finger Print Reader has been purchased and installed.

[3] This selection is only available if the optional license for the Badging Software has been purchased and installed.

[4] This selection is only available if the optional license for the Card Import Utility has been purchased and installed.

Reports



Use this menu option to customize and generate History Reports, Database Reports, and Visitor Reports[5].

History Reports (Ctrl+H)

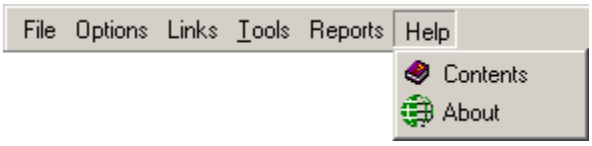
Reports are explained later in Chapter 7.

Database Reports

Reports are explained later in Chapter 7.

[5] This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

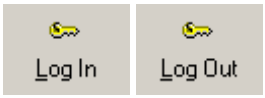
Help



Use this menu option to display information regarding your Integra32™ software version, the licensing of the software, as well as dealer information.

Create a text file in the site folder (e.g. default) named rbh.ini (as shown below) to display dealer information in the *About* screen. Up to nine lines of information (DealerInfo#) can be included.

Toolbar Buttons



Login/Logout

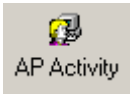
Press this button to log in or log out of Integra32™ system.

Status

Press this button to change the *Command Screen* to display the status of access points, inputs, outputs, and panels.

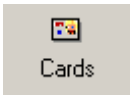
Alarms

Press this button to change the *Command Screen* to display alarm messages, time and date of alarm and operator ID. This change will take place automatically when an Alarm Event occurs.



AP Activity

Press this button to toggle on and off the Access Point Activity screen pop-up.



Cardholders

Press this button to launch Integra32™'s cardholder window to program new cards or edit existing cards.

Visitors[6]

Press this button to launch the Integra32™'s visitor window to administer visitors in the system.

DVR[7]

Press this button to launch the DVR module to monitor the CCTV system live.

[6] This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

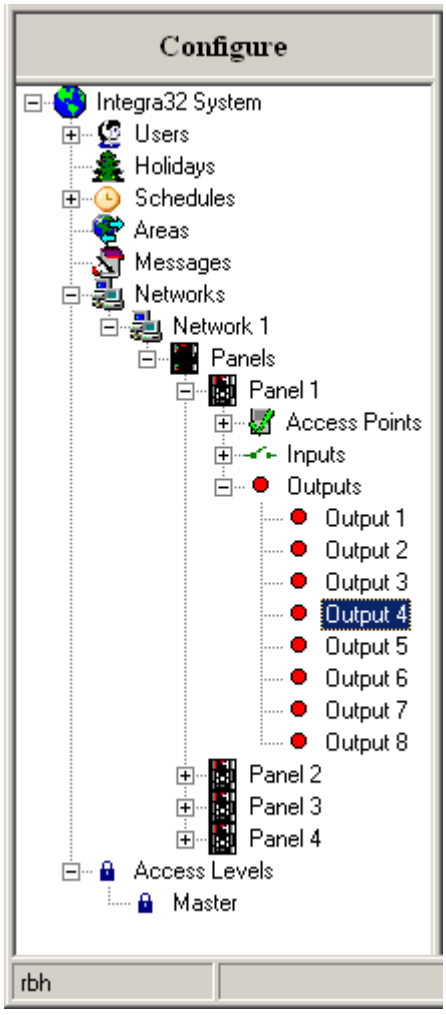
[7] This selection is only available if the optional license for the DVR Interface has been purchased and installed.

Help

Press this button to get online help.

Database Screen

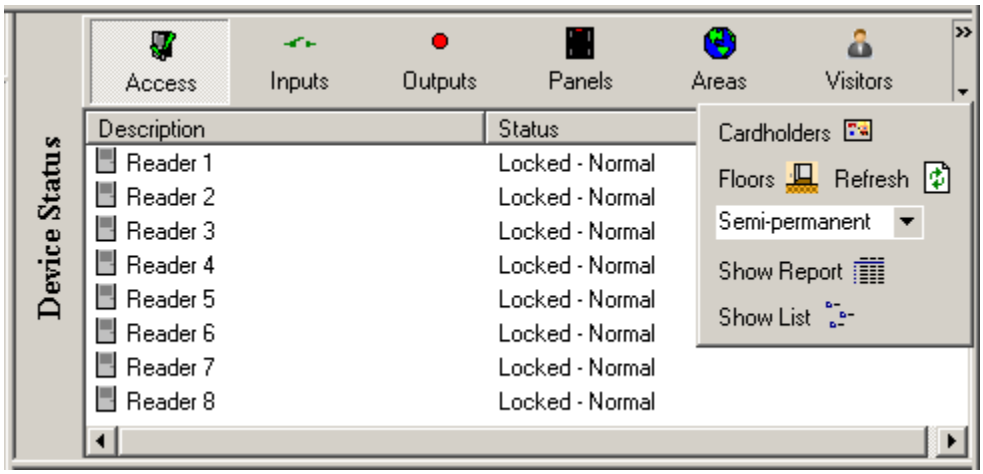
The system is configured for a particular installation from this screen. Setup and programming of hardware devices (*IRC-2000*), and programming of all records such as, access levels, schedules, and holidays are done here, with the exception of cardholders.



Up to sixteen networks can be configured and up to thirty-two panels can be configured, for each Integra32™ system. These panels can be distributed across the sixteen networks, as you like with no more than sixteen panels on any one network. A maximum of thirty schedules, each with up to eight periods, can be added to the existing schedules (*Never and Always*). The system is capable of handling up to forty holidays and one hundred messages.

Device Status Screen

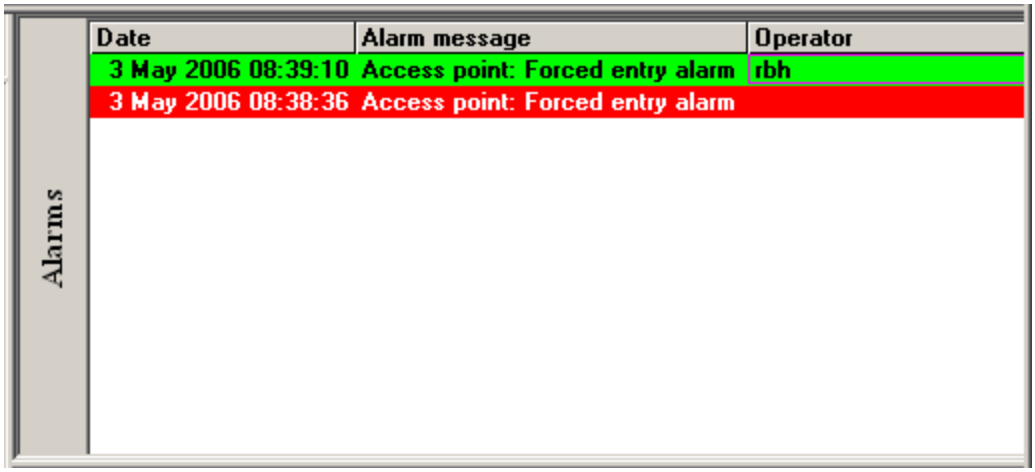
This screen gives the operator control of the system through Operator Commands, and it provides viewing of the status of the items that have been selected (e.g. *Access Points, Input Points, and Output Points*).



Status for items shown is in real time. Items are updated as events change keeping the operator up to date.

Alarms Screen

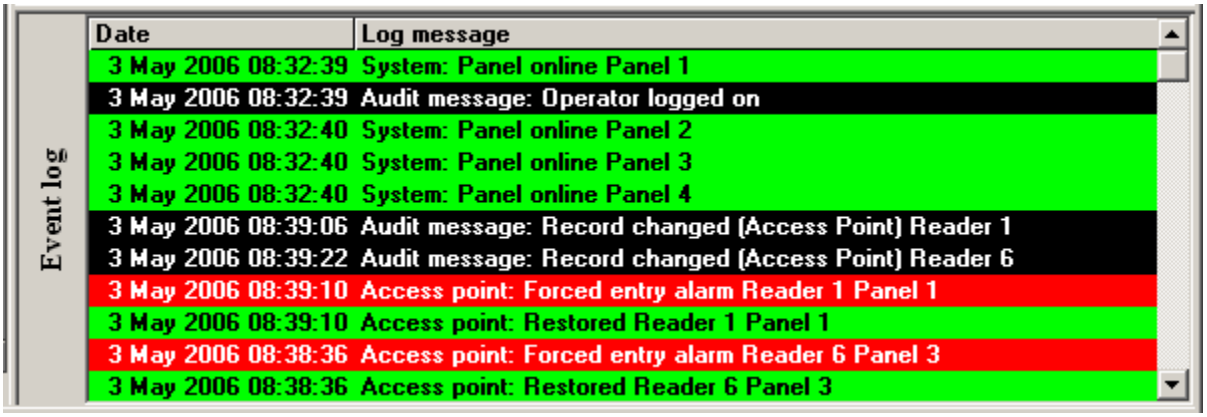
This screen appears in the same pane in place of the *Status Screen*. From here alarms are acknowledged and cleared.



Instruction messages can be obtained from the *Details* of the alarm, and actions taken can be noted there as well.

Event Log Screen

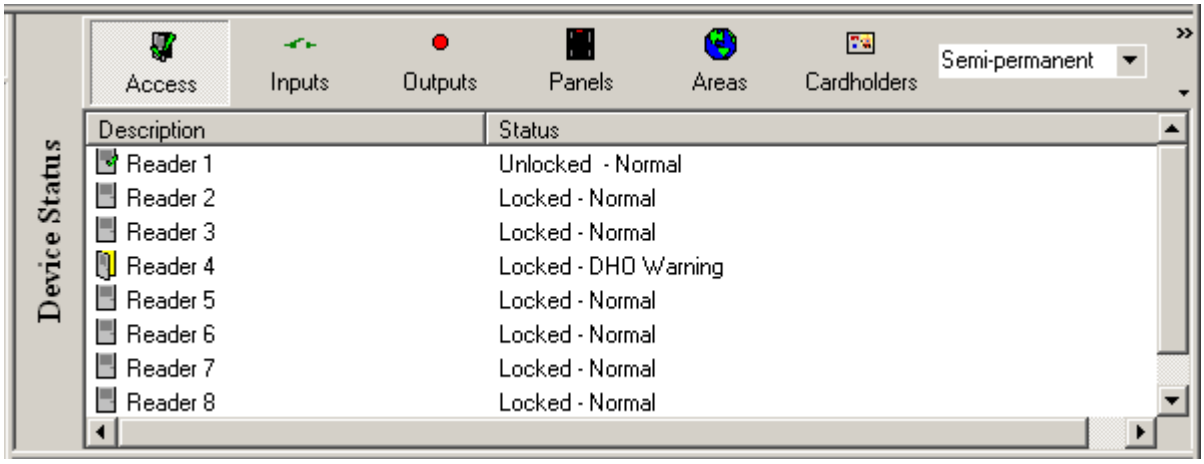
This screen displays all system activity such as cardholder activity, input activity, output activity and panel activity. All system messages are also displayed here.



All the messages shown here are also saved to *History* and can be retrieved through History Reports.

Chapter 3
Command Screen

From the *Command Screen* the operator can issue commands, as well as view status. Commands can be sent to access points, inputs, outputs, and panels. Areas can be cleared and cardholders can have their area set or cleared. Alarms cab be acknowledged and cleared.



Device Status

Clicking on the *Status* button on the toolbar of the main screen will change the *Alarms Screen* to the *Device Status Screen*. From the *Device Status Screen* the operator can lock and unlock doors, arm and disarm inputs, and switch on and off outputs. The status is displayed in real time, but only for those devices that have reporting enabled. The operator can turn messages off for certain events and no history will be logged for those events, but the status of devices will not be affected.

The first six buttons will bring up Access Points, Inputs, Outputs, Panels, Areas, and Cardholders respectively. The seventh button is used to update/verify the status of the items shown.

How to Execute a Command

All operator commands are executed in the same manner.

1. Click on the appropriate button on the *Device Status Screen* toolbar to load the desired devices.
2. From the list of items (*Input, Output, or Access Point etc*.), select the item(s) you want to control. Clicking on the first item, then holding down the **Shift** key and clicking on the last item in the range can choose a group of items. Select non-sequential item groups by holding down the **Ctrl** key and clicking on each desired item.
3. Set the command type to permanent, semi-permanent or timed.
4. Right click on the Item(s) highlighted and then choose a command from the list provided.

The command is then immediately sent to the appropriate IRC-2000 controller(s) for execution.

Command Type

From the drop down menu select one of the three options available for command type.

Permanent

Permanent commands are used to perform actions and to manually override system operation. When the status of an input, output or access point is changed by a permanent command, the scheduler no longer controls the device. For example, if a door is normally armed from 6:00 p.m. to 8:00 a.m. by the scheduler and a permanent command is issued to arm the door, the door will remain armed forever and will not be disarmed by the scheduler.

A permanent command remains in effect until cleared by a second operator command or fresh files are downloaded to the controller.

Semi-Permanent

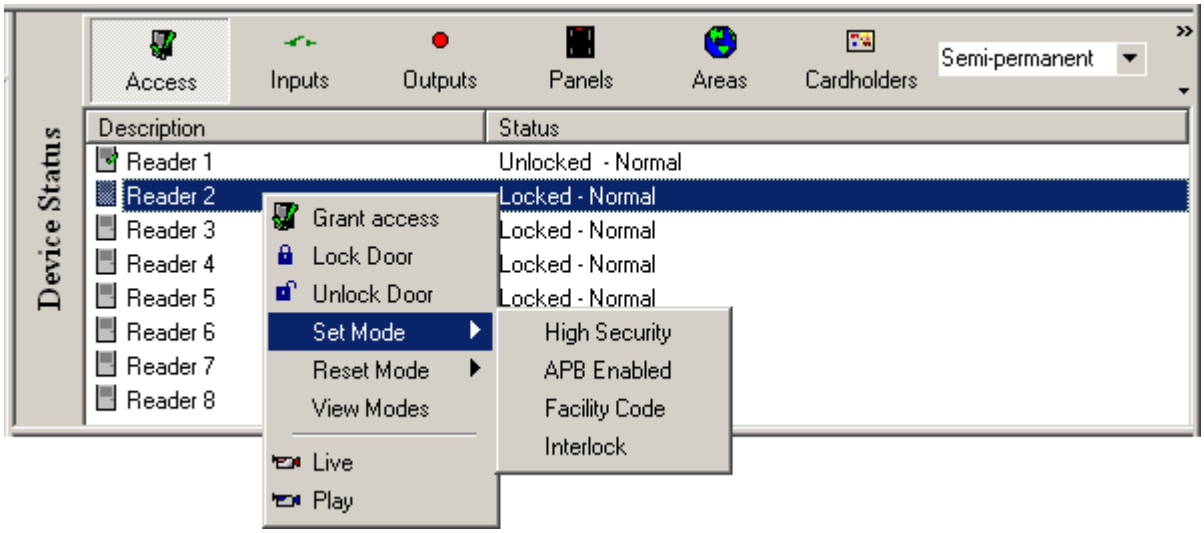
Semi permanent commands are executed like permanent commands but do not override operation of the scheduler. In the above example of the door armed by scheduler between 6:00 p.m. and 8:00 a.m., if a semi permanent command is issued at 4:00 p.m. to arm the door, the command is executed. The scheduled operation remains unaffected and on the next day at 8:00 a.m. the door will disarm and revert to the normal arming schedule.

Timed

Timed commands allow an action to be performed for a specified duration. For example, turn on an output for five minutes. The time can be specified from 1 to 127, seconds or minutes.

Access Points Commands

Clicking the Access Points button on the *Command Toolbar* depicts the status of Access points on the *Device Status Screen*.



The following commands for Access points are available by right clicking the selected Access points.

Commands

Grant Access

Unlock the access point for the duration of the access point *Unlock Time*. This command has the same effect on an access point as presenting a valid card.

Lock

Lock an access point or access point group on a permanent, semi-permanent, or timed basis.

Unlock

Unlock an access point or access point group on a permanent, semi-permanent, or timed basis.

Set Mode

The access point has several operating modes that are normally controlled by the scheduler. The operator can override the scheduler and manually control these modes.

Reset Mode

Reset Mode button is used to turn off the option turned on in Set mode.

High Security

In High Security mode, only cards with high security privileges, may gain access at this access point.

APB Enabled

Antipassback is an access control feature that prevents cardholders' misuse, by putting certain restrictions on the use of their cards. When the Antipassback feature is enabled, cardholders must present their card for entry to and exit from all areas. Antipassback prevents a cardholder from using his/her card twice at the same access point.

Facility Code

Use this option to turn on/off the Facility Code mode, when the system checks only the Facility Code portion of the card code. All cards with valid Facility Codes will be granted access. This feature is typically used when the system is being configured for the first time and the cardholder information is not entered in the database.

Interlock

With this feature enabled a door will not be unlocked if the other door is opened. The open door must be closed before the other door will grant access.

View Mode

Select this option to view all the modes available and their status.

Live[8]

Select *Live* to display live video from the CCTV camera associated with the selected access point.

Play[9]

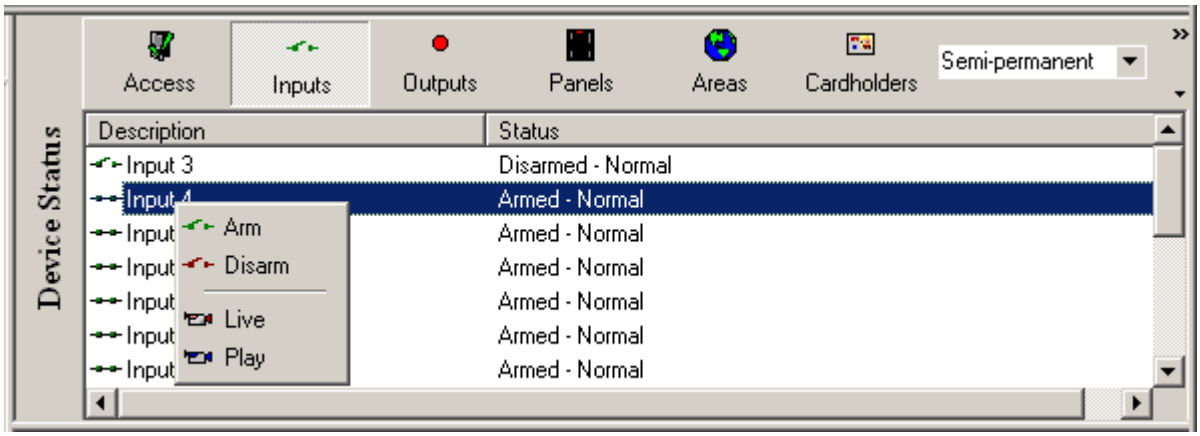
Play will bring up a DVR history selection screen so that video connected to an event for the chosen access point can be played back.

[8] This selection is only available if the optional license for the DVR Software has been purchased and installed.

[9] This selection is only available if the optional license for the DVR Software has been purchased and installed.

Input Points Commands

Clicking the *Input Points* button on the *Command Toolbar* depicts the status of input points on the *Device Status Screen*.



The following commands for Input points are available by right clicking the selected Input points.

Commands

Arm Input

Arm the input. When an input is armed, an alarm is generated if the input is violated. In the case of a door, opening an armed door generates an alarm.

Disarm Input

Disarm an input. While an input is disarmed, no alarm is generated when the input is violated. In the case of a door, opening the door while disarmed does not generate an alarm. The system however will still generate and log a "door opened" event and report it to the *Log Screen*.

Live[10]

Select *Live* to display live video from the CCTV camera associated with the selected input point.

Play[11]

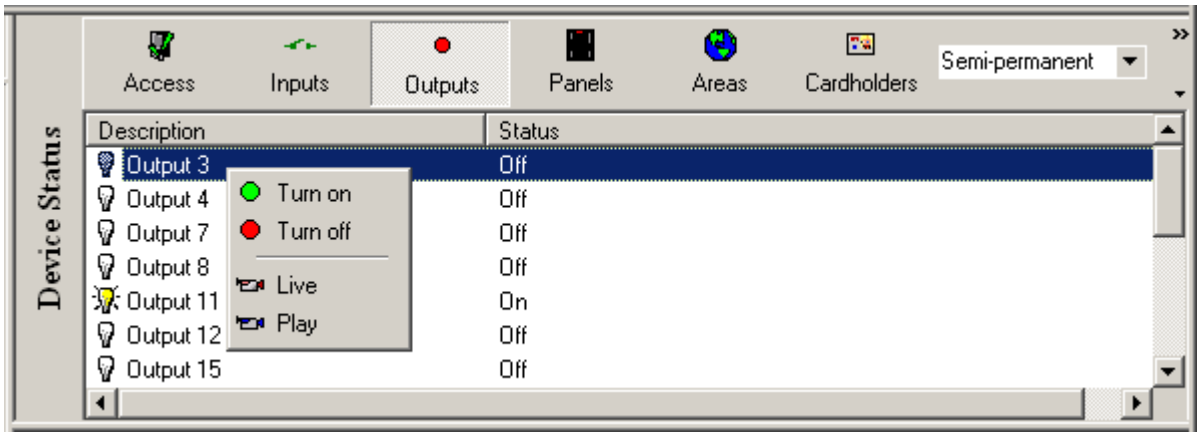
Play will bring up a DVR history selection screen so that video connected to an event for the chosen input point can be played back.

[10] This selection is only available if the optional license for the DVR Software has been purchased and installed.

[11] This selection is only available if the optional license for the DVR Software has been purchased and installed.

Output Points Commands

Clicking the *Output Points* button on the *Command Toolbar* depicts the status of output points on the *Device Status Screen*.



The following commands for output points are available by right clicking the selected *Output Points*.

Commands

Turn On

Turn on an output.

Turn Off

Turn off an output.

Live[12]

Select *Live* to display live video from the CCTV camera associated with the selected output point.

Play[13]

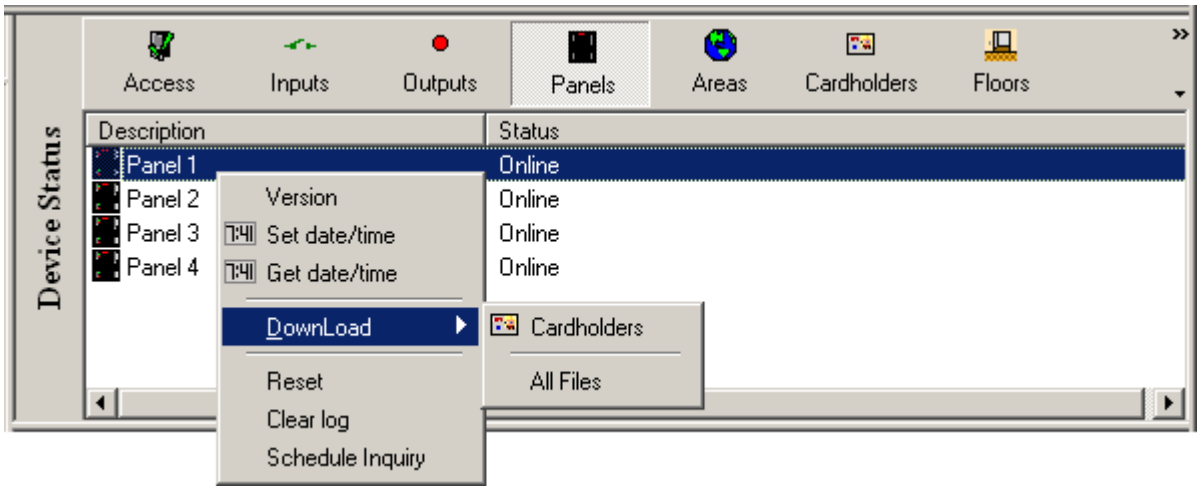
Play will bring up a DVR history selection screen so that video connected to an event for the chosen output point can be played back.

[12] This selection is only available if the optional license for the DVR Software has been purchased and installed.

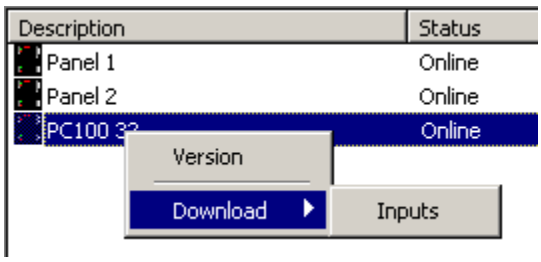
[13] This selection is only available if the optional license for the DVR Software has been purchased and installed.

Panels Commands

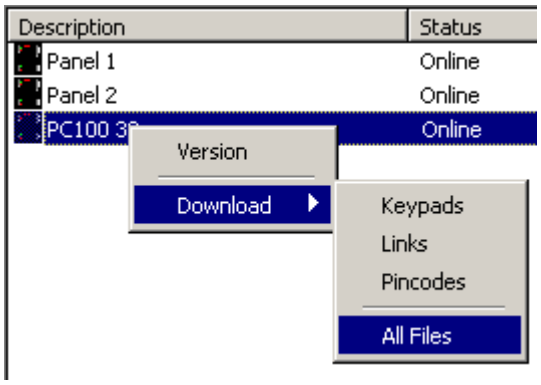
Clicking the *Panels* button on the *Command Toolbar* depicts the status of panels on the *Device Status Screen.*



IRC2000 or URC2000



PC100 (Summit or Risco Group)



PC100 (Bosch)

Commands IRC2000 & URC2000

The following commands for panels are available by right clicking the selected IRC2000 and/or URC2000 panel(s).

Version

The *Version* queries all or selected IRC-2000 and/or URC2000 for the firmware version they are running. The version number will be displayed on the *Log Screen*.

Set Date/Time

Click on the *Set Date/Time* to launch the *Set Panel Date/Time Screen*.

- The *Get Local* button is used to retrieve the current date and time settings from the PC's internal clock.
- The Set button is used to upload the selected *Date/Time* settings to the selected IRC-2000 and URC2000 controllers.
- The *Close* button is used to close the *Set Panel Date/Time Window*.

Get Date/Time

This command queries the controller for its current date and time, and displays it on the *Log Screen*.

Download

The *Download* function allows the operator to manually repopulate the IRC-2000 and/or URC2000 memory from the database on the server. Select any of the listed files to download or select the *All Files* option to download all files.

Download messages are posted to the log as files are sent, verifying the number of records sent in each file. Card records are sent individually and will indicate the card number, and whether it was added or deleted. (*Edited cards are displayed as added*.)

If the panel is offline at the time of the download the files that failed to download will be logged on the *Log Screen*. When the panel comes back on line the download will be executed then, again logging the files that are downloaded.

Clear Log

The *Clear Log* option clears the event log of all or selected controllers. The database portion of memory is untouched. The results will be displayed on the *Log Screen*.

Schedule Inquiry

This query is used to find out the current state of the time schedules. It will list on the *Log Screen* which schedules are on and which is off.

Commands PC100 (Summit or Risco Group)

The following commands for panels are available by right clicking the selected PC100 (Summit or Risco Group) panel.

Version

The *Version* queries the selected PC100 for the firmware version it is running. The version number will be displayed on the *Log Screen*.

Download

The *Download* function allows the operator to manually repopulate the PC100 memory from the database on the server. Click on '*Inputs'* to download the data.

Download messages are posted to the log as files are sent, verifying the number of records sent for the file.

If the panel is offline at the time of the download any files that fail to download will be logged on the *Log Screen*. When the panel comes back on line the download will be executed then, again logging the files that are downloaded.

Commands PC100 (Bosch)

The following commands for panels are available by right clicking the selected PC100 (Bosch) panel.

Version

The *Version* queries the selected PC100 for the firmware version it is running. The version number will be displayed on the *Log Screen*.

Download

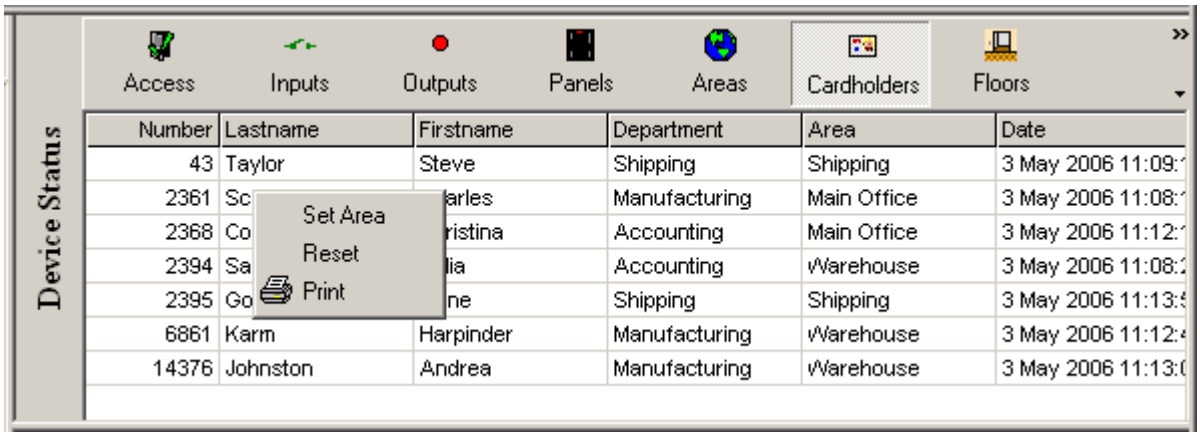
The *Download* function allows the operator to manually repopulate the PC100 memory from the database on the server. Select any of the listed files to download or select the *All Files* option to download all files.

Download messages are posted to the log as files are sent, verifying the number of records sent in each file.

If the panel is offline at the time of the download the files that failed to download will be logged on the *Log Screen*. When the panel comes back on line the download will be executed then, again logging the files that are downloaded.

Area and Cardholder Commands

Clicking either the *Areas* or the *Cardholders* button will bring up a selection window. From the *Areas* selection window you can choose the area or areas you wish to view. The *Cardholders* selection window allows you to choose from the list of cardholders. The display will show a list of cardholders based on your selections. You will see the area the cardholder is logged into and the date/time they were logged into that area.



The following commands for areas are available by right clicking the selected cardholder.

Commands

Set Area

Set Area is used to change the area that a cardholder is logged into. This may be necessary if a cardholder get into an area without reading into that area.

Reset

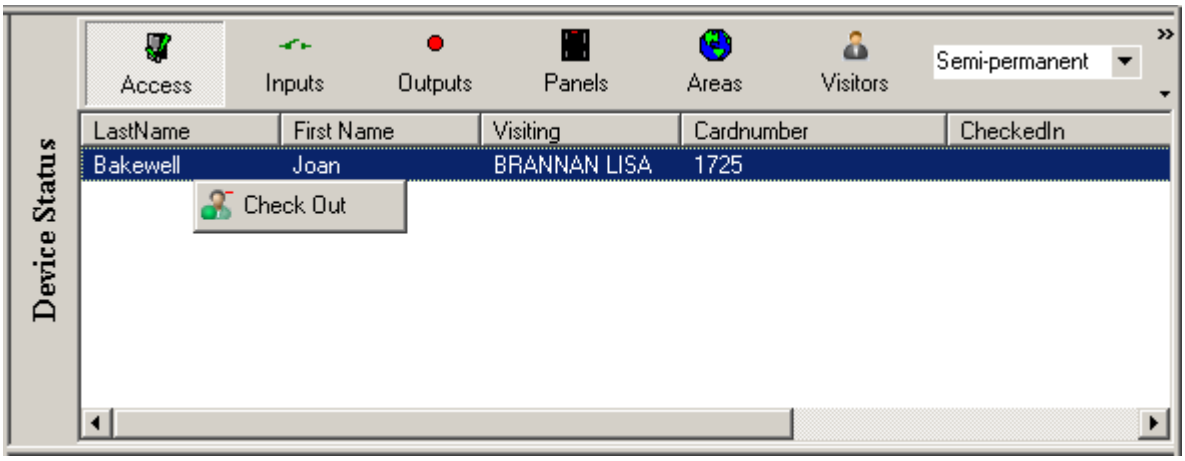
The Reset command will clear the area the cardholder is in. The cardholder will not be logged into any area; therefore the next card read cannot violate antipassback.

Print

The Print command will produce a printed report showing the data provided in the status pane. It will show all of the cardholders displayed and the areas they are in.

Visitors[14]

Clicking the *Visitors* button on the *Command Toolbar* will display the visiting cardholders and who they are visiting.

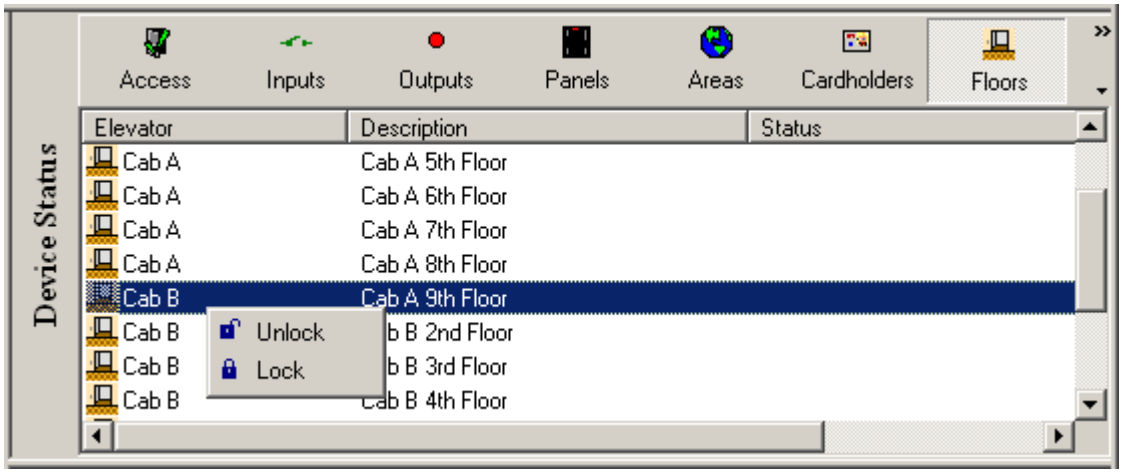


Check Out

Click *Check Out* to check-out the selected visitor.

Floors

Clicking the *Floors* button on the *Command Toolbar* depicts the status of floor outputs on the *Device Status Screen*.



Unlock

Unlock will release the floor button in the cab so that allow anyone may access the floor.

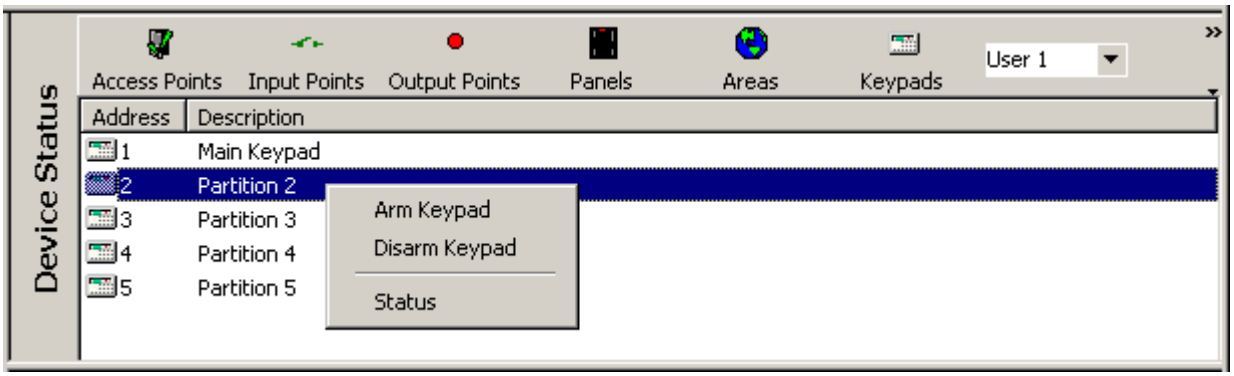
Lock

Lock will energize the floor output and disconnect the floor button in the cab. A card with the appropriate access level can release the floor temporarily.

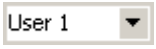
[14] This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

Keypad Commands

If you have installed a PC100 for Bosch you will have a Keypads icon on the Status button bar. Click on this icon to bring up the list of Bosch keypads.



Commands



Select the name of the PIN code that the command is to be issued by.

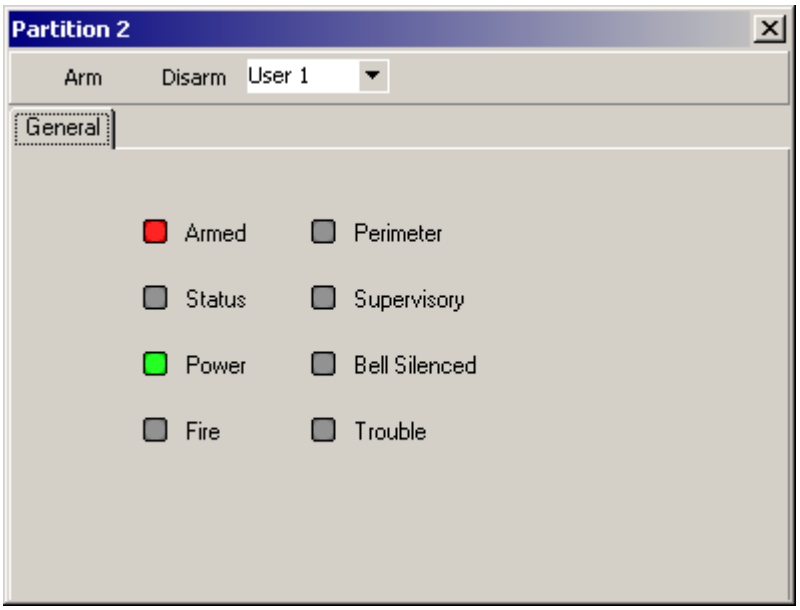
Arm Keypad

Arm the selected keypad with the selected PIN code.

Disarm Keypad

Disarm the selected keypad with the selected PIN code.

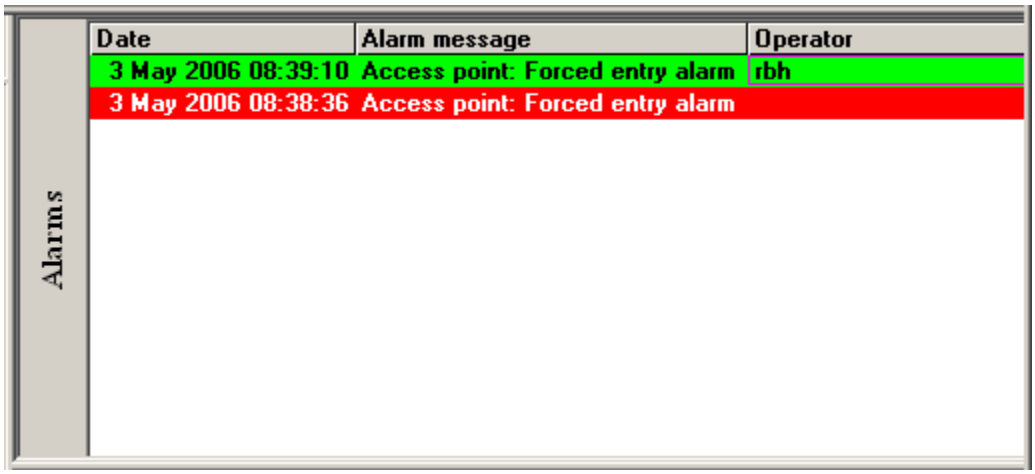
Status



LED keypad status will be displayed in this window. Arm & disarm commands can also be issued from here.

Chapter 4
Alarms Screen

The *Alarms Screen* displays alarm events and pops up automatically when the *Alarms* option is turned on in the toolbar of the main screen.



Acknowledge/Unacknowledge/Clear

Right clicking the alarm event on the *Alarms Screen* gives the option to acknowledge the Alarm. Right clicking on an Acknowledged Alarm gives the options to either clear or unacknowledge the alarm. Once an alarm is acknowledged, only the operator that acknowledged that alarm can clear it.

A maximum of one hundred and fifty alarms can be held in the alarm buffer. Any alarms received when the buffer is full are logged to history but do not get sent to the *Alarms Screen*.

Alarm Details

The user can see the details of an alarm event in *Alarm Details Window* by double clicking the alarm event in the *Alarms Screen*.

Date

This box shows the date and time that the alarm occurred.

Age

The age of an alarm is the number of seconds since the alarm happened.

Status

Status shows whether the alarm has been acknowledged.

Alarm

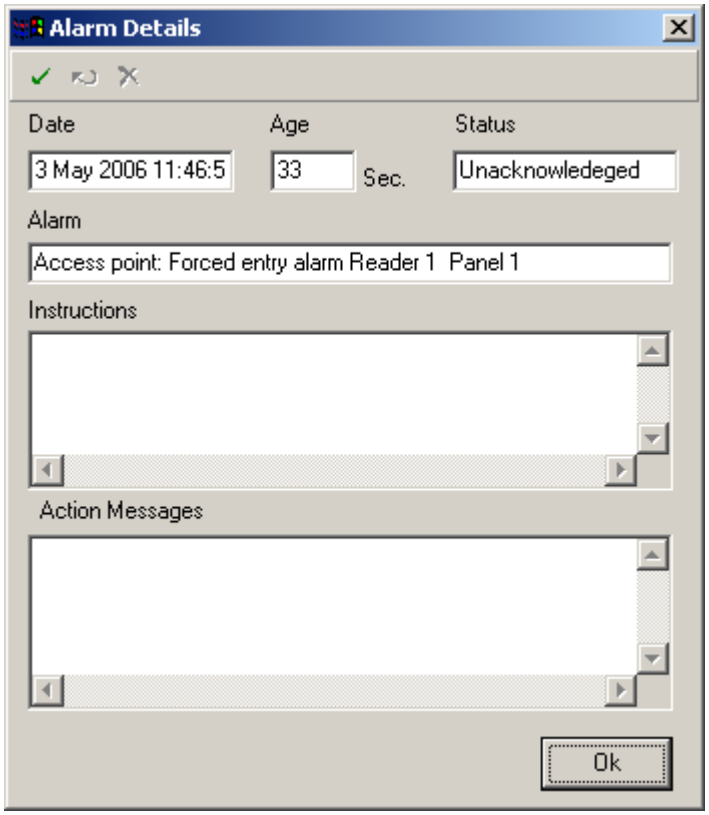
Alarm provides a description of the alarm.

Instructions

This box will display instruction messages assigned to the alarm.

Action Messages

The operators can enter their own message into this box indicating what action was taken because of this alarm.



Acknowledge

Acknowledge the highlighted alarm with this selection.

Acknowledge All

Acknowledge all of the alarms in the Alarm Window with this selection.

Unacknowledge

Unacknowledge the highlighted alarm with this selection.

Clear

Clear the highlighted acknowledged alarm with this selection.

Clear All

Clear all of the acknowledged alarms in the Alarm Window with this selection.

Live[15]

Select *Live* to display live video from the CCTV camera associated with the selected alarm event.

[15] This selection is only available if the optional license for the DVR Software has been purchased and installed.

Chapter 5
Programming

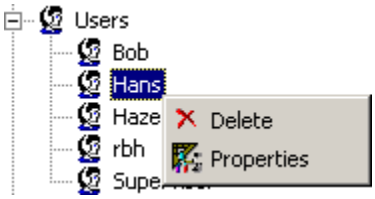
Click on the + sign to expand the tree view of your Integra32™ system in the *Database Screen*. Click on the – sign to compress it. Double clicking the description will either expand or compress the view depending on the sign associated with the text. Items that do not have a sign (+ *or* –) associated with them will take you to their properties when they are double clicked.

Right clicking on the different selections will bring up small menus. From these menus you can add, delete, or go to properties for the selected item. Right clicking the access point, the input, or the output will not bring up a menu (*there are no options to select*), but will expand the tree view instead.

Integra32 Database

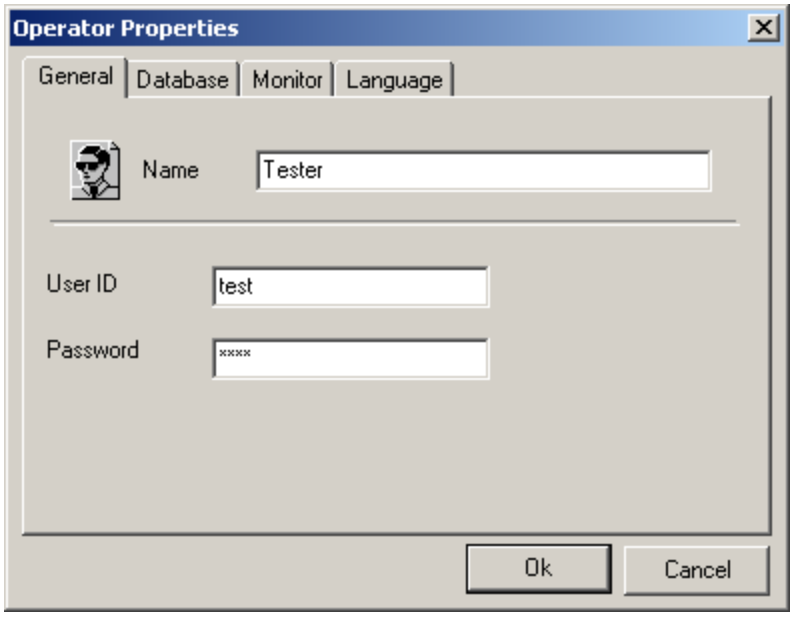
Users

The Integra32™ system comes with user 'rbh' by default, with password 'password'. Additional Users/Operators can be added and configured the in the *Database Screen*.



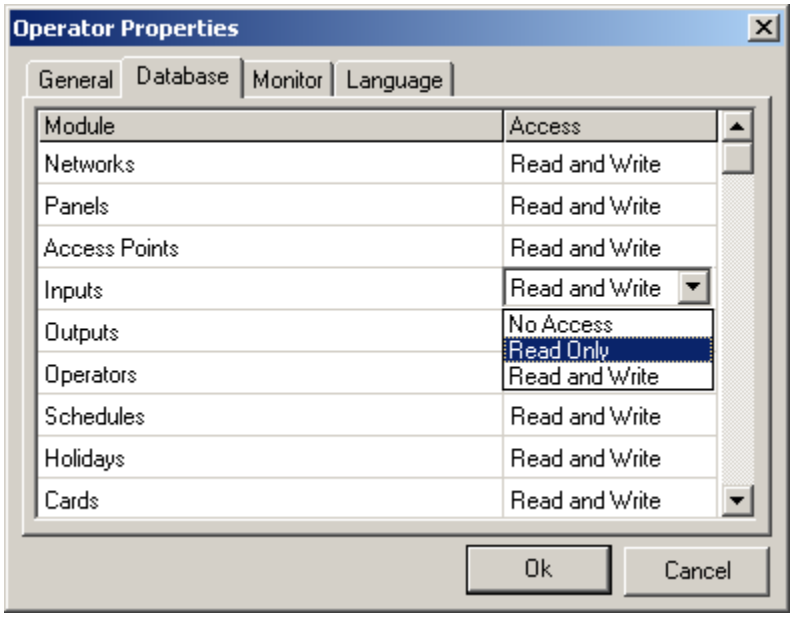
General

Name, user ID and password can be changed/entered in the *General* tab of the *Operator Properties Window*.



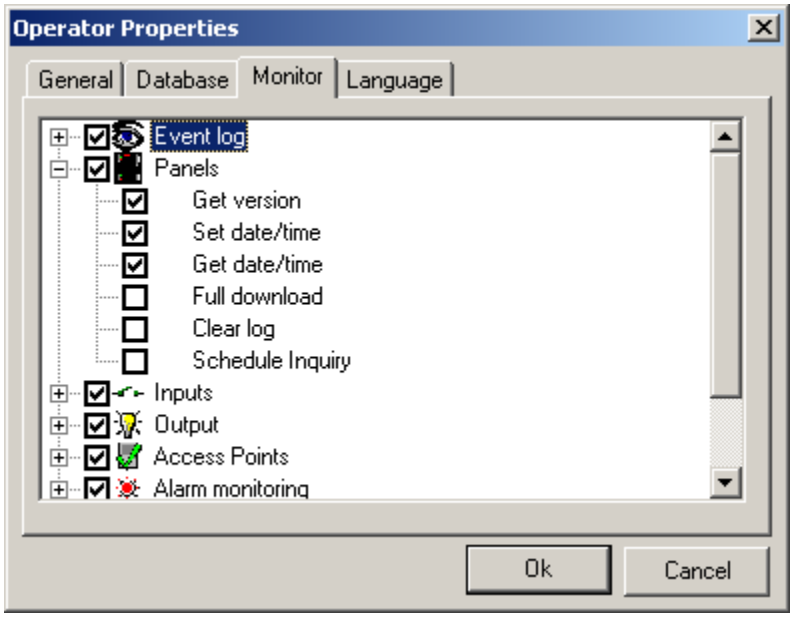
Database

The access to database can be defined/changed in the *Database* tab. Access to each module of the database can be chosen as 'No Access', 'Read Only', or 'Read & Write'. (*For some items 'Read Only' access may not be relevant. If 'Read Only' access is selected for these items their access will actually be 'Read & Write'.*)



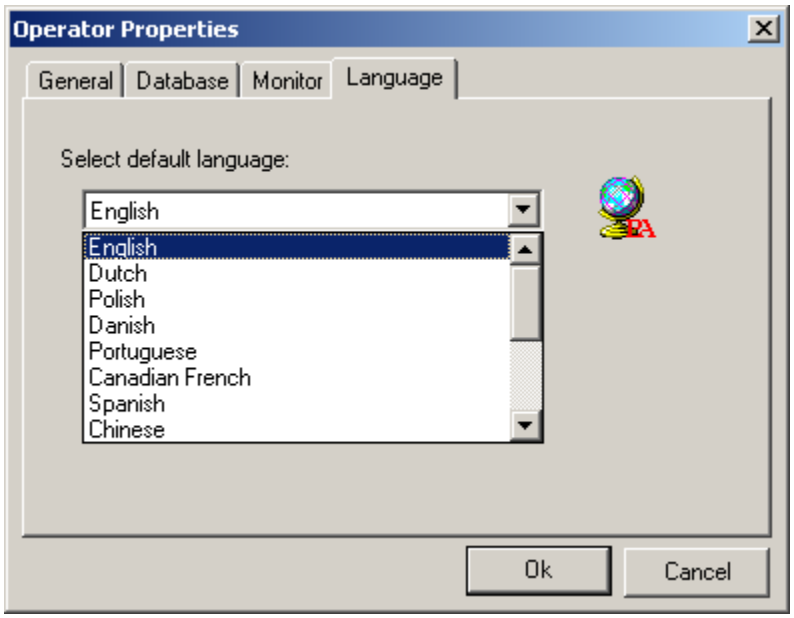
Monitor

Access to commands used in the *Device Status Screen* and the *Alarms Screen* can be defined/changed in the *Monitor* tab. Check commands that the user is to have access to and uncheck commands that he/she is not to have access to.



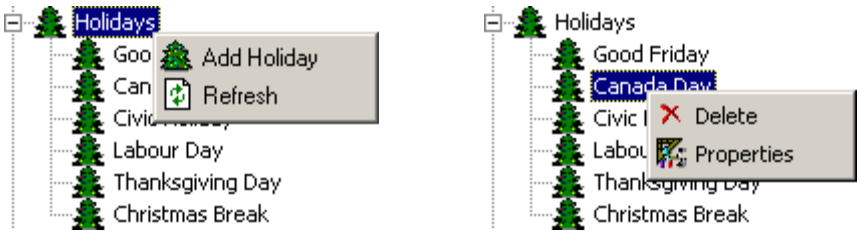
Language

The language the system will operate in, for this operator, is selected in the *Language* tab.



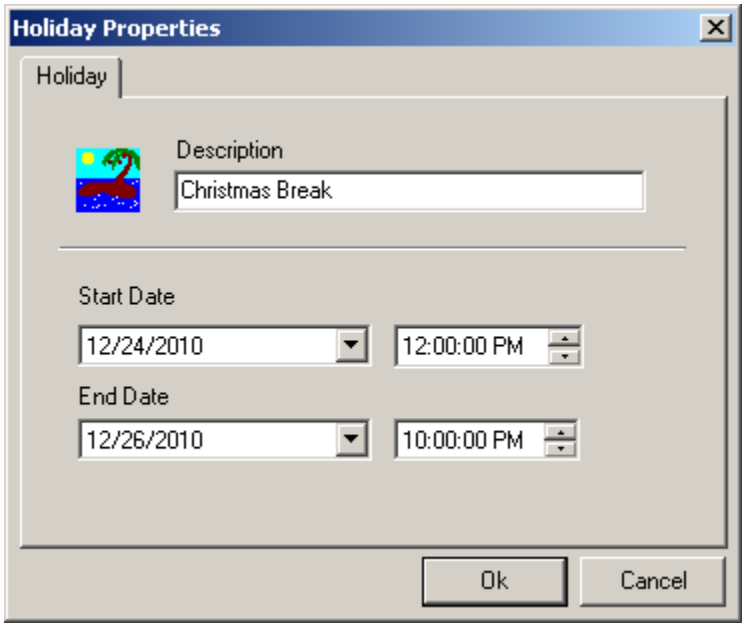
Holidays

Up to forty holidays can be assigned.



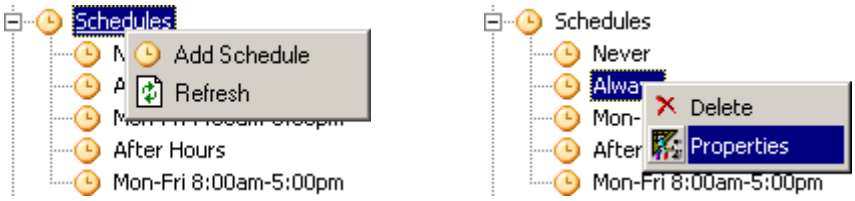
You can edit/create the name of a holiday and the date(s) of a holiday in the *Holiday Properties*. You can *Select a Date* the holiday starts on and an *End Date* for the holiday. Any date designated as a holiday, will replace the regular day of the week for the day specified. (*E.g. Good Friday 2 April, 2010 as far as schedules are concerned this day will not be a Friday it will be H1*.)

Start and end times can also be specified for the holidays. In the example shown below the holiday starts on 24 December 2010 at noon. Up until noon the day is Friday, at noon the day becomes H1. The holiday remains until 10:00pm on 26 December 2010 when the day of the week changes from H1 to Sunday.



Schedules

Before cardholders are entered, any additional *Time Groups* that are required should be programmed. Up to thirty-two schedules can be programmed for Integra32 system.

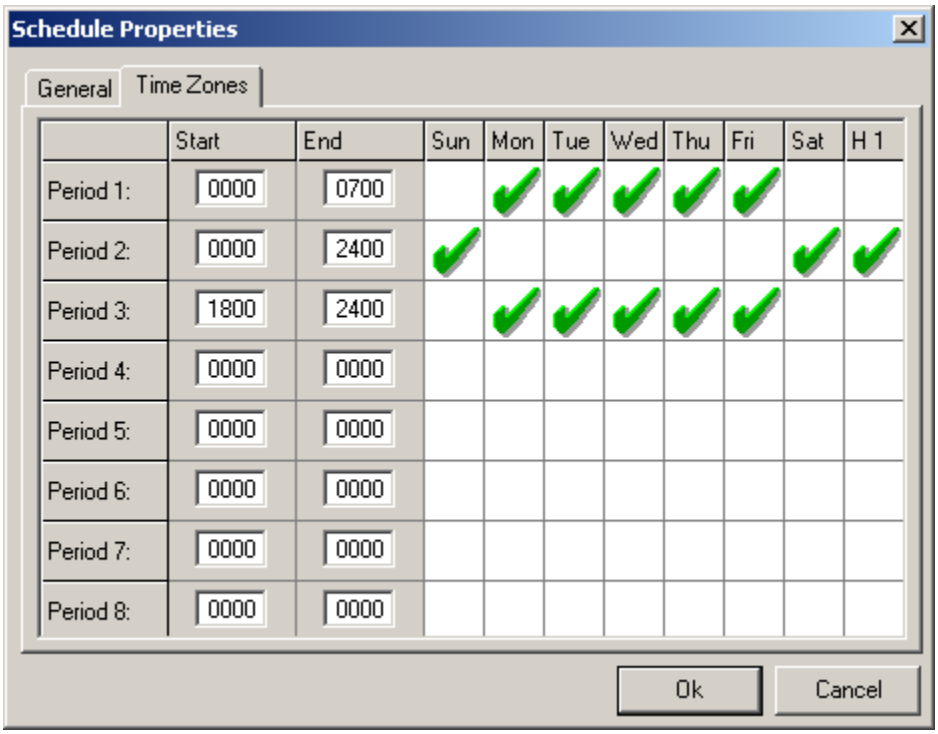


General

Change the *Description* of the Schedule under the *General* tab of the *Schedule Properties Window*.

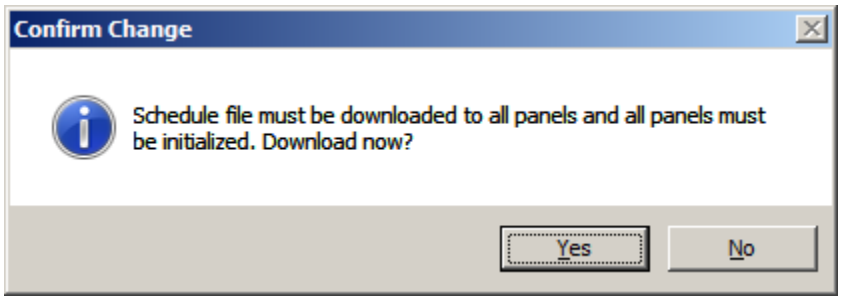
Time Zones

Program the *Time Zones* for the *New Schedule* in the *Time Zones* tab of the *Schedule Properties Window*.

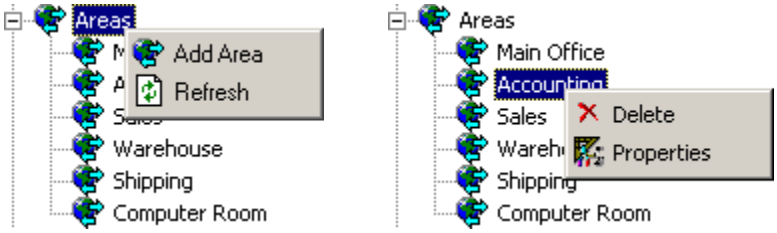


- Eight time periods can be programmed.
  - Click to check or uncheck a day for the period.
  - End time must be later than start time.
  - Valid times are from 00:00 to 24:00, (*even though 24:00 is never actually reached* [*it represents the end of the day*]).
    - Schedules that cross, midnight will require two periods. One to go up to 24:00 on the first day, and a second to start at 00:00 of the next day.

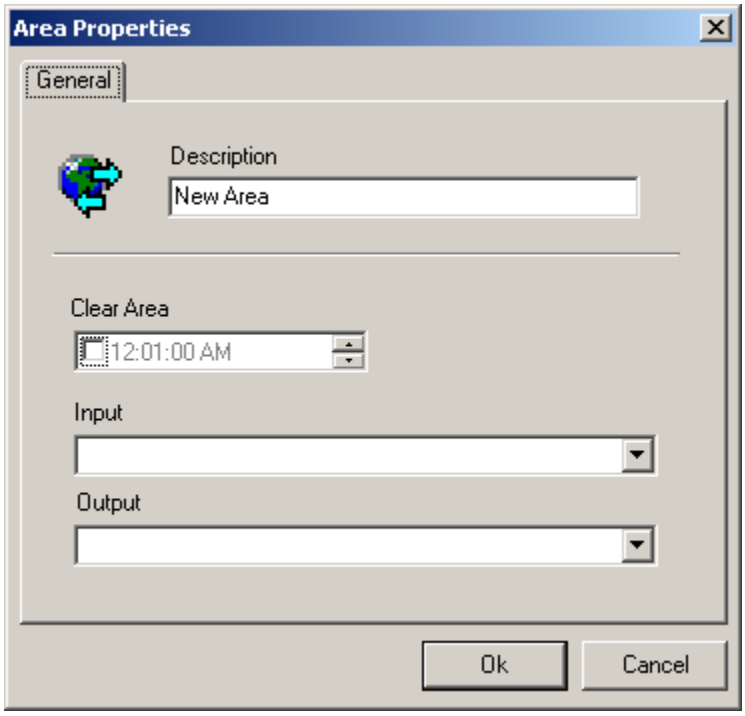
After you create a new schedule, edit an existing schedule, or delete a schedule, you will be asked if the changes are to be downloaded and the panel initialized now or will it be done later.



Areas

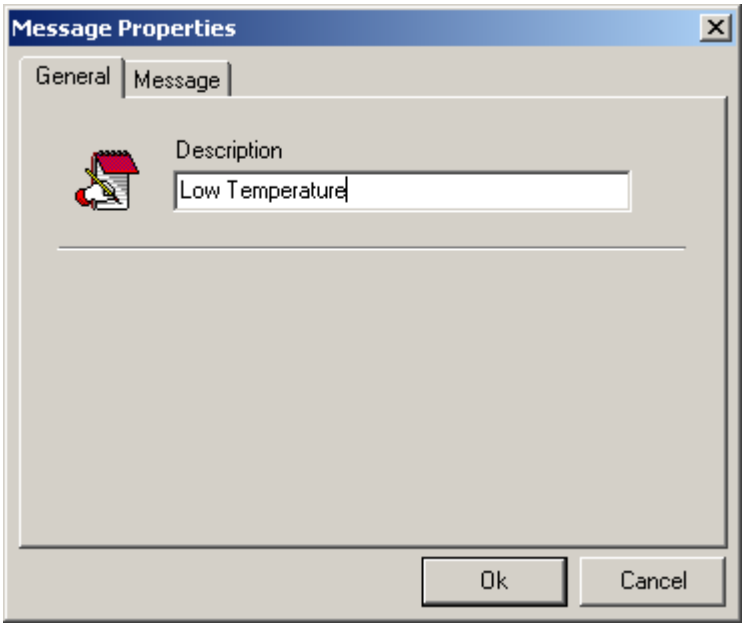


In the *Area Properties window* the name of the area is entered. Access points from which a cardholder can enter or exit the area define the actual area. A '*Clear Area*' time can also be entered here. As well an input and an output (*both general purpose*) can be chosen. To print out a report of all the cardholders in the area simply put the input into alarm. The output will be turned on when there are no cardholders in the area, it must be turned off manually (*operator command*).



Messages

Messages/Instruction that operators need to follow under certain circumstances can be created and saved here.



General

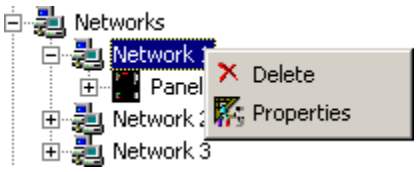
Under the *General* tab of the *Message Properties Window* message descriptions can be edited.

Message

The message is entered under the *Message* tab.

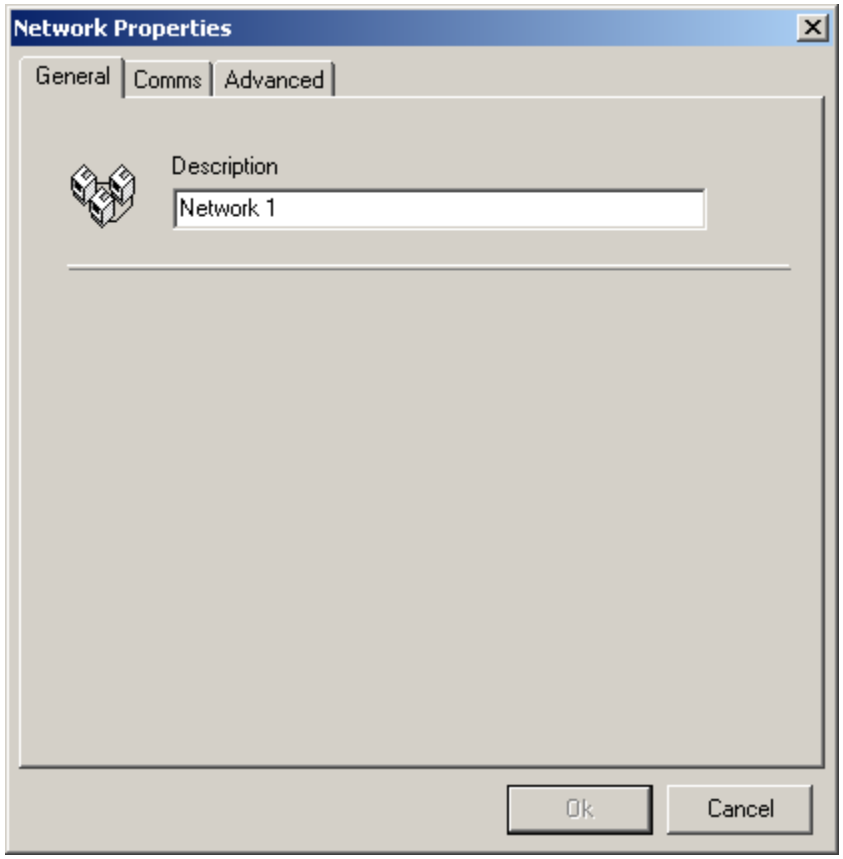
Networks

Up to sixteen networks can be connected on the Integra32™ system. The description of each *Network* can be changed in the *Description* box under the *General* tab of the *Network Properties Window* for each network. Under the *Comms* tab, properties of the port are configured. Choose one of the four options available for *Port Type*.



General

Under the *General* tab of the *Networks Properties Window* network descriptions can be edited.



Comms

Poll Retries

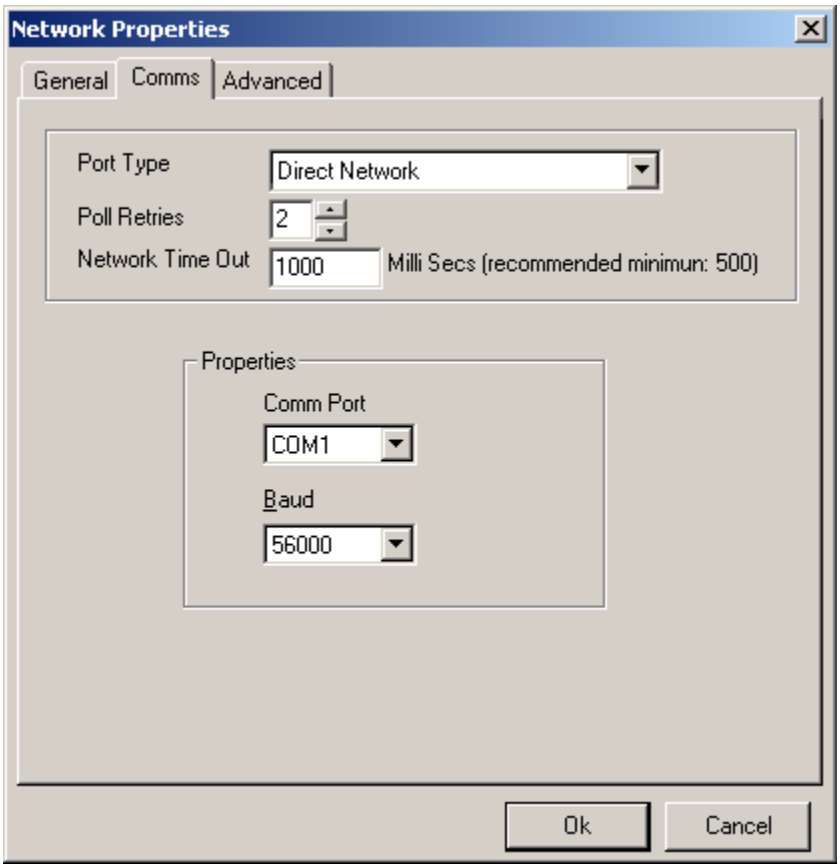
Poll Retries is the number of times the Integra Server will poll a panel before declaring the panel offline and moving on to poll the next panel.

Network Time Out

Network Time Out is the amount of time the Integra Server will wait for a response before polling again.

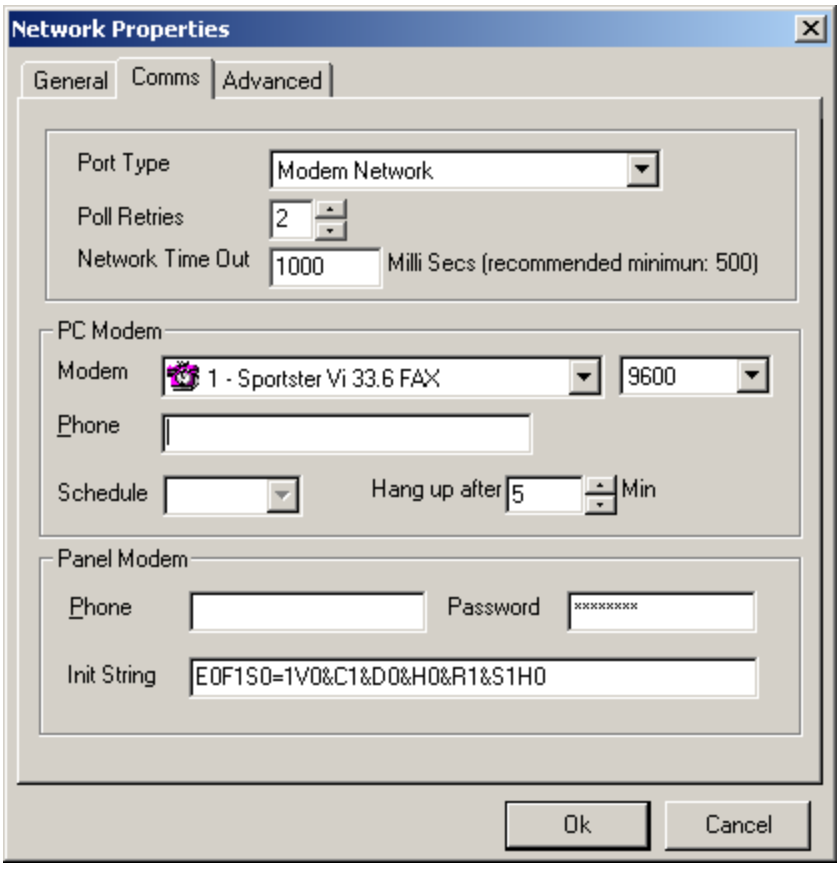
Direct Connect

The controller network (*IRC-2000*) is connected directly to the PC serial port, via either RS232 or a USB-485 module.



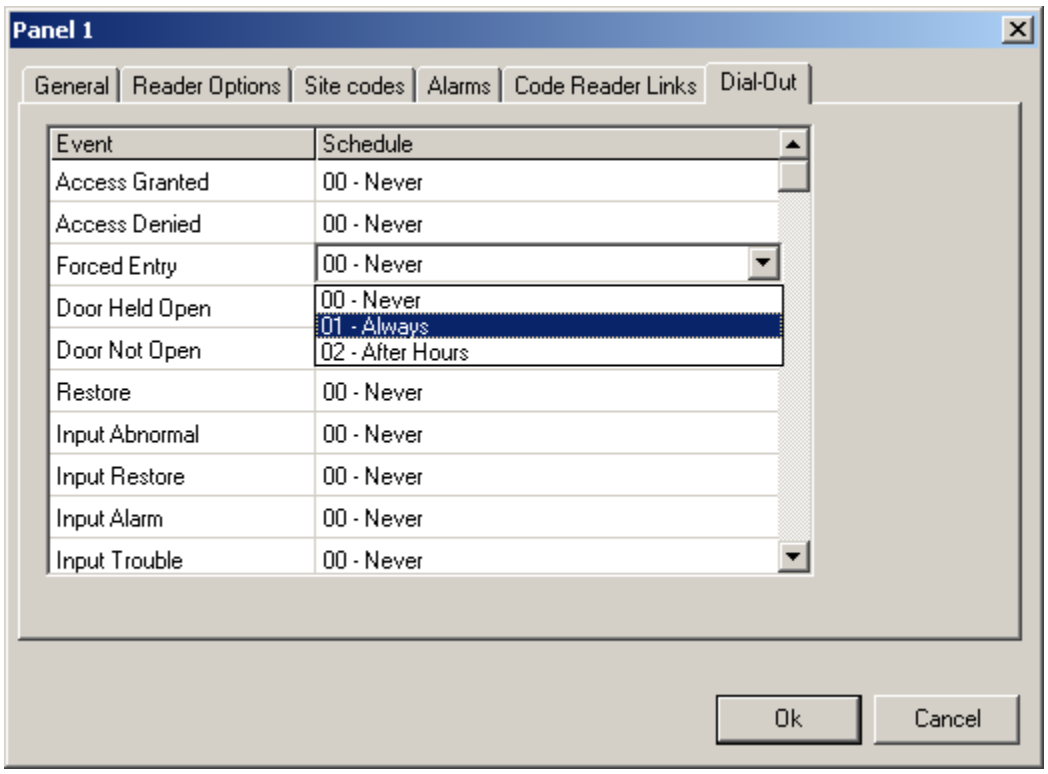
Modem Connect

The controller network (*IRC-2000*) is located remotely and is connected to the PC via dial up modems.



Select a modem and configure it in the *Control Panel* to a maximum baud rate equal to that set at the panel (*e.g. 9600*). Enter the phone number for the network (*to be called by the PC*) and the call back phone number (*for the panel to call*). Auto hang-up time can be set in minutes (*the number of minutes with no activity*).

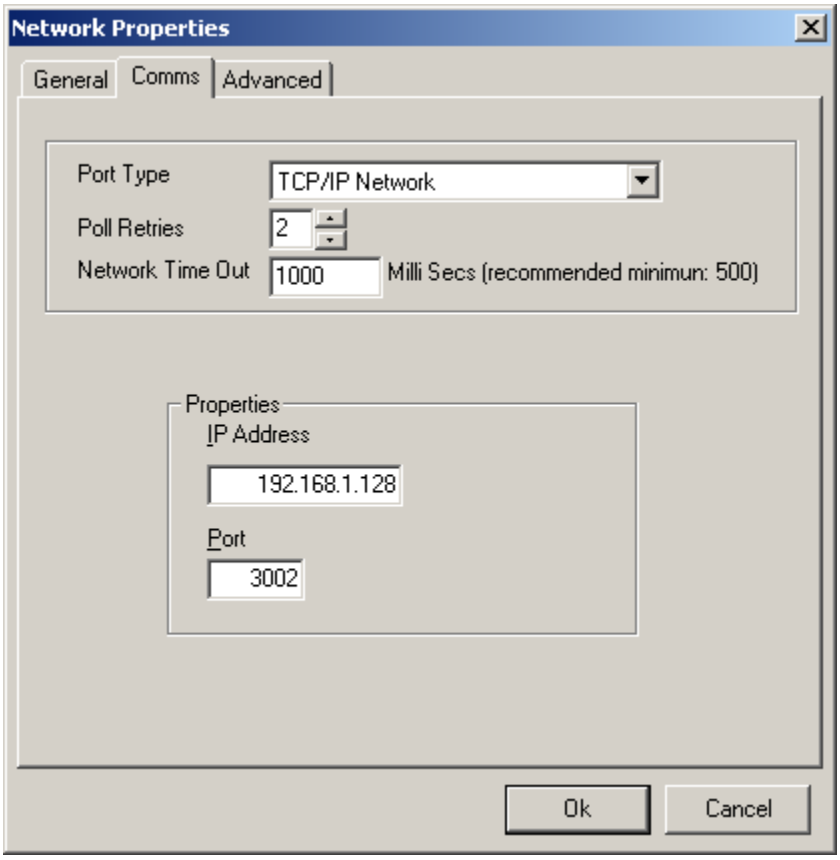
The call back criteria are set under the *Dial-out* tab of each panel. Which events will cause the panel to call up the PC can only be set in the panels of a modem network.



To reset the password, connect the panel directly to the Integra32™ system and execute a full download to the panel.

Ethernet Connect

The controller network (*IRC-2000*) is connected to the PC through a standard Ethernet network.



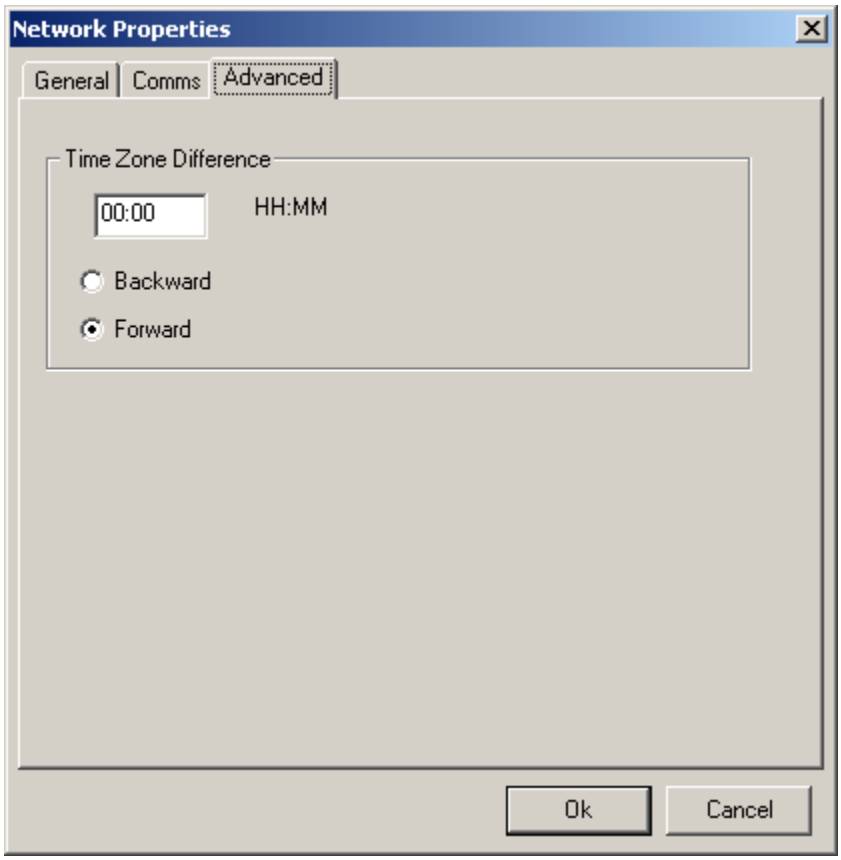
For an Ethernet connection to work **TCP** must be installed on your computer.

Enter the specific address and proper port value for the Ethernet interface assigned to the network. (*Enter a port value of which must match programming of Interface.*)

Advanced

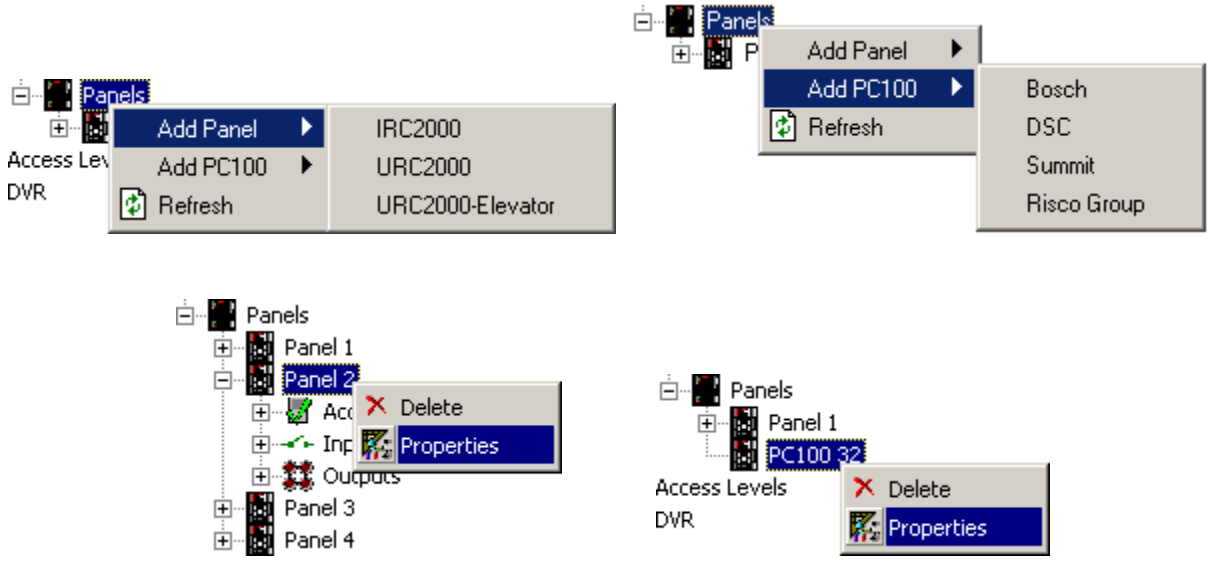
Time Zone Difference

If a network is located in an area within a different time zone you can set the difference here. Set the number of hours either ahead or behind of the time where the server is located.



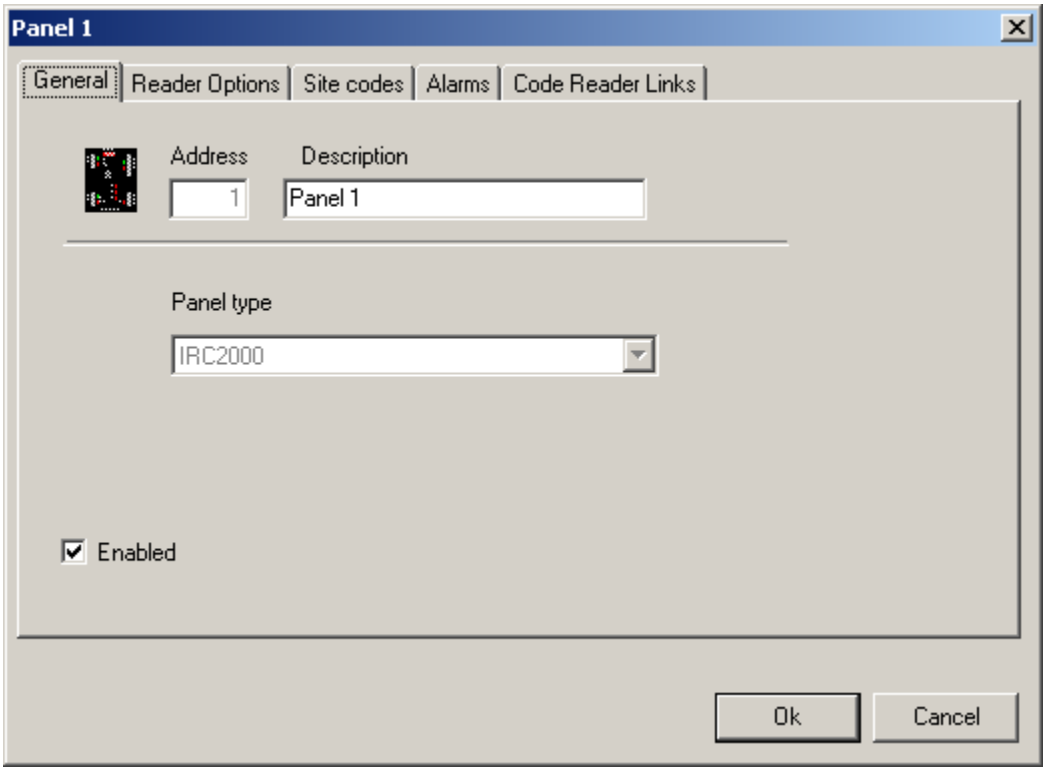
Panels

Up to thirty-two panels in total can be connected to the Integra32™ system.



IRC2000 or URC2000

General



Address

The address is selected at the time creation and cannot be edited later.

Description

To change the default description simply type over it.

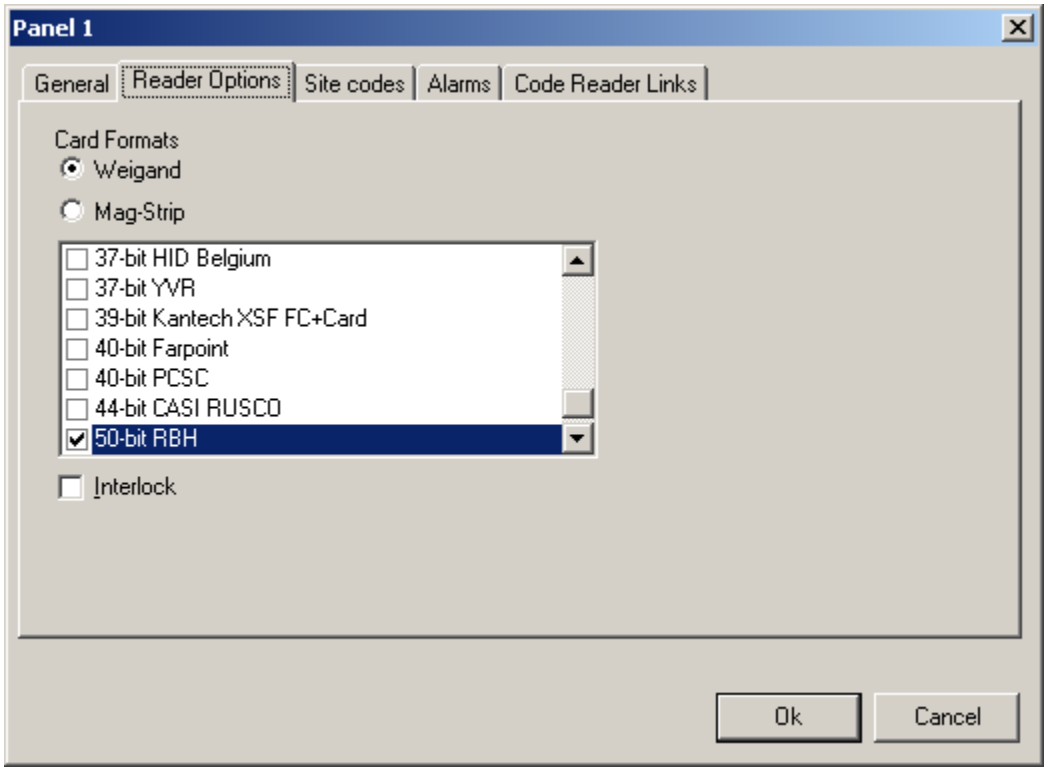
Panel Type

The panel type is chosen when the new panel is added and cannot be edited later.

Enable

If the enable check box is not checked then the panel will not be shown in the status screen. All Access Point, Inputs, and Outputs under that panel will also be disabled. Disabled items are still in the database but are not considered to be part of the system.

Reader Options



Card Format

This is where the card format is selected (*only a limited number of formats are supported- list provided*).

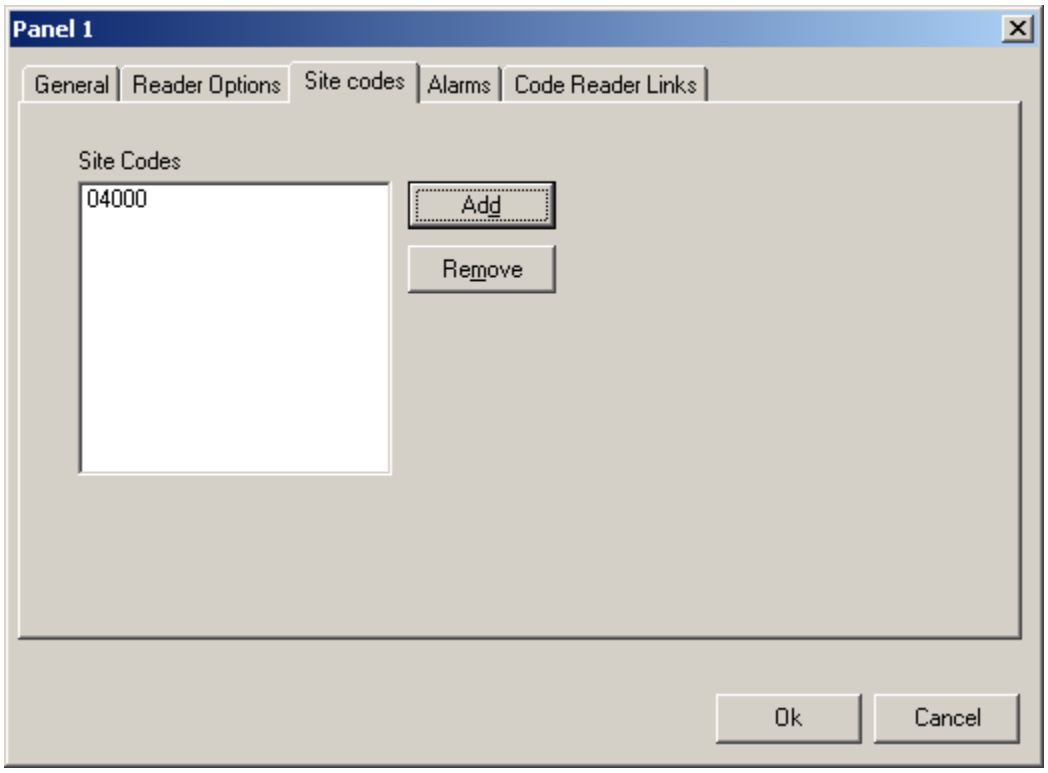
Interlock

With Interlock checked only one of the two doors on the one panel may be opened at a time. If one door is open then access will not be granted at the other door until the first door is closed.

Site Codes

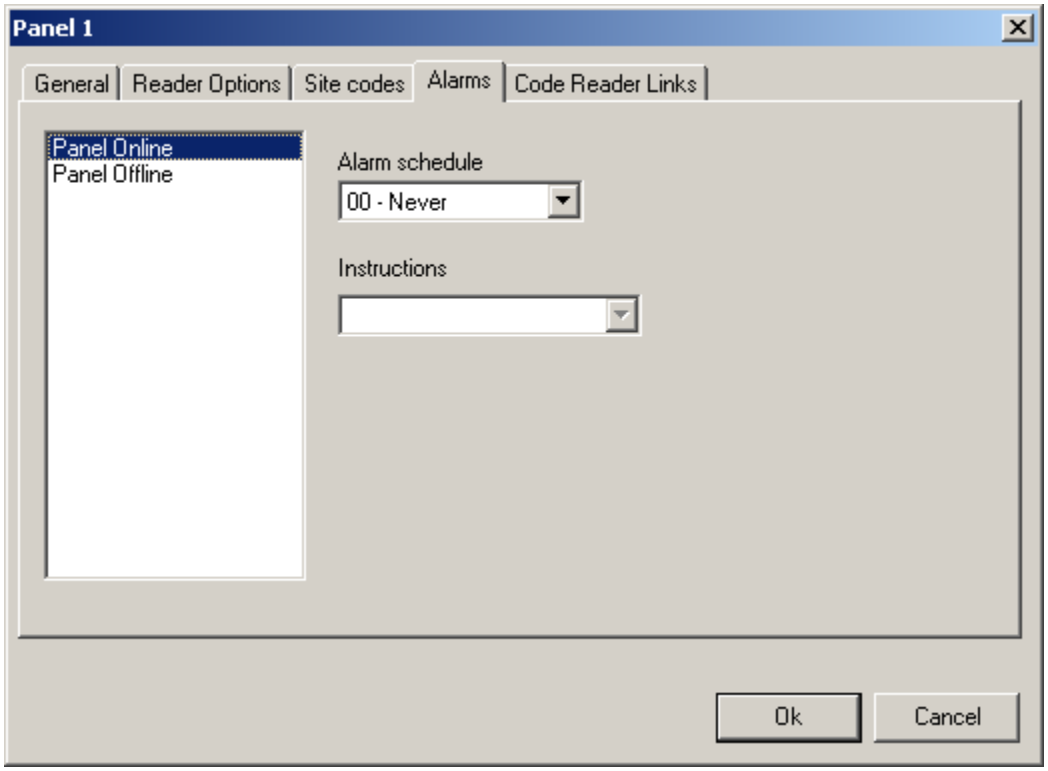
Under the *Site Codes* tab the facility code to be used by the IRC-2000 is entered. (*Each IRC-2000 panel will support up to five facility/site codes*.)

Leading zeros are not required when entering a site codes, even though the display does show them.



Alarms

Under the *Alarms* tab the schedules are set for when *Panel Online* and *Panel Offline* cause an alarm. An instruction message can be assigned to these alarms as well from this tab. Instruction messages are created elsewhere.

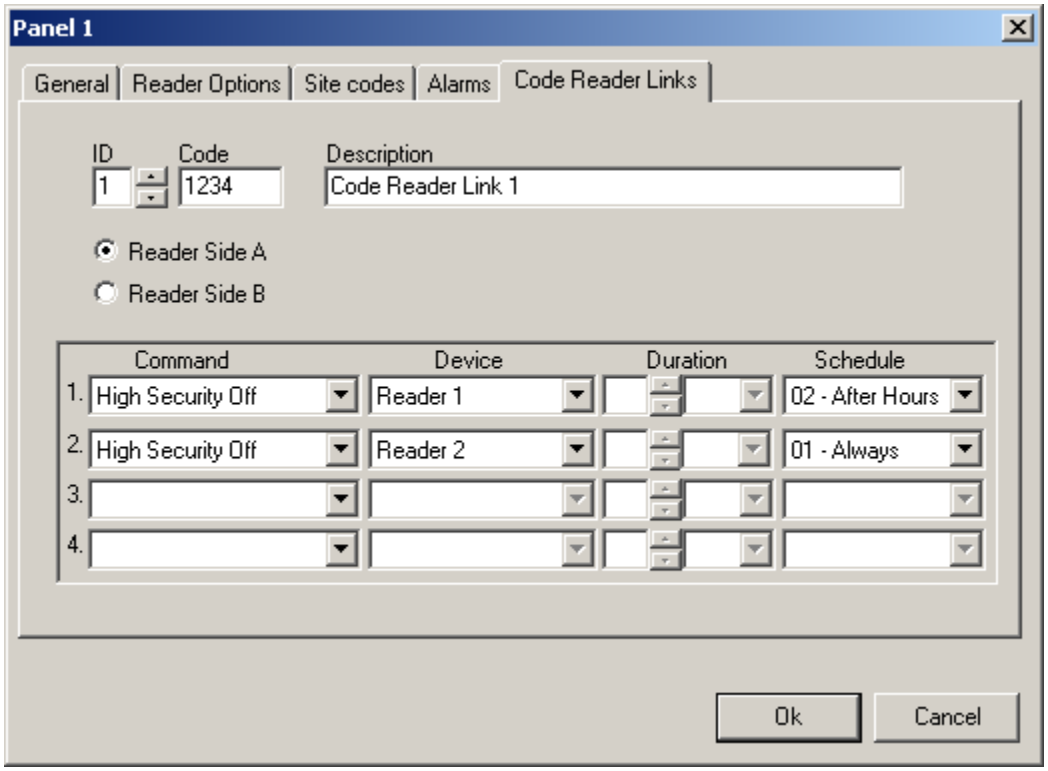


Code Reader Links

Code reader links can be linked to one or multiple inputs, outputs, and access points on a local basis. A single access code with a card read is capable of invoking different links dependent on which access point it is presented at. This linking is done at the controller level without the Host PC online. A combination card reader and keypad is needed to utilize this function. The programmed link is executed for the appropriate key code after a grant access has been executed at the specified access point. In the example below 'Code Reader Link 1 (*High Security Mode off for both Reader 1 & Reader 2*)' will be executed after a grant access and a key code entry of '1234', on the side A reader of Panel 1.

Code reader links are used primarily in HVAC control, lighting control and intrusion alarm control systems where it is necessary to control inputs, outputs, and other access points from a single card read. With code reader links, the same cardholder can perform different functions at each access point. In addition, every cardholder can perform a unique function at every access point. Further, links can have several entries, allowing execution of multiple commands at each access point when a card is presented.

This window contains the following fields and options:



ID

The number of the code reader link may be system generated by pressing up and down button or user-defined. A maximum of 16 code reader links can be generated.

Code

Put in the code number. These codes can be in the range of 1-32767.

Description

The user specified description of link.

Choose one of the two radio buttons- Reader side A or B on which code reader link has to be executed.

Then as with local links you choose which event on what device will cause the link to be executed. You can choose up to four things to have happen with one code.

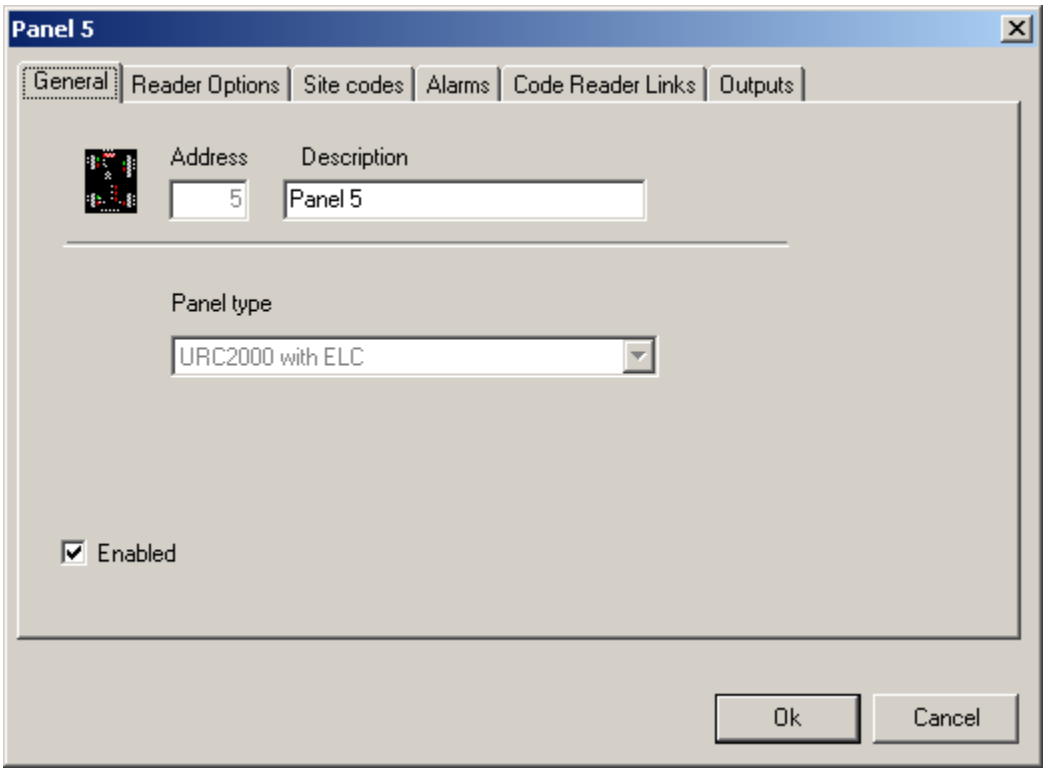
Dial-Out

This tab is visible only if the Network to which the panel is connected is Modem Network. (*For more information see page 38.*)

URC2000 with ELV

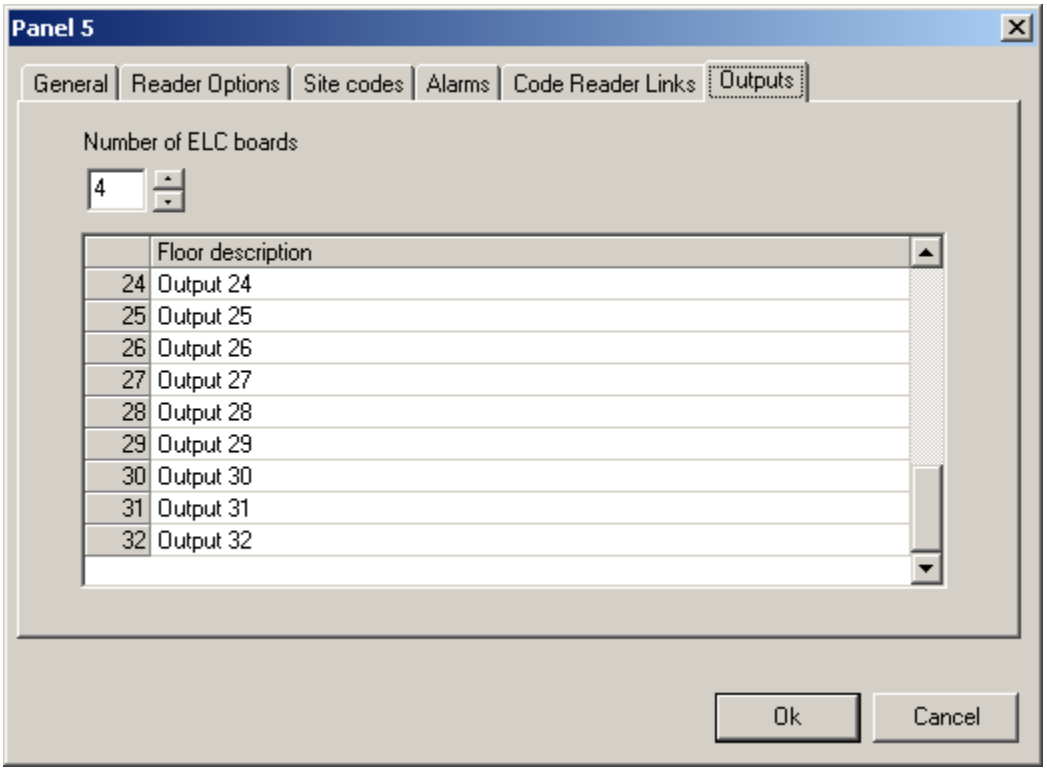
The first five tabs (General, Reader Options, Site Codes, Alarms, & Code Reader Links) are *almost* the same as above for the regular URC-2000. URC-2000 Elevator panels have a sixth tab (Outputs). These outputs, on the ELC-08 boards, are the only outputs that can be used for elevator control.

Reader ports on an elevator board can be used for either elevator control or access control. When an access point is used for elevator control change all of its default inputs and outputs to general purpose, the elevator reader won't need them. If you use the access point for access control it won't have all of the features that access points on other panels have. Access points on an elevator control will not have 'Deduct Usage', 'Disable Forced Entry', 'Unlock Schedule', 'First Person Delay', 'RTE Bypass DC', 'Report RTE', 'Antipassback', or an 'Alarm Shunt' output. Timed commands will act as semi-permanent commands. Extended Unlock time will be fixed at thirty seconds, Door Held Open warning will be fixed at twenty seconds, and Door Held Open alarm will be fixed at thirty seconds.

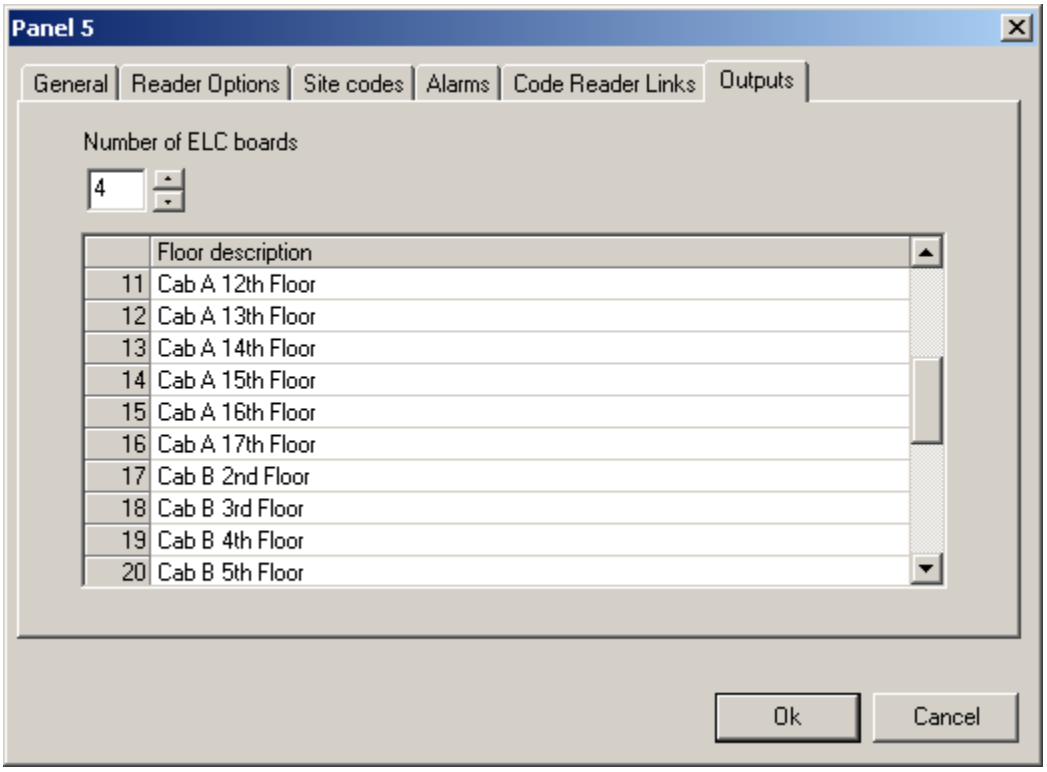


Outputs

Up to four eight-output relay boards may be used with each URC2000 Elevator Control. These outputs may be split between the two readers of the panel or all outputs may be used with just one reader. Use the scroll buttons to select the number of relay boards that are connected.



Rename the outputs for your convenience.



PC100

IRC2000 panels connected along with the PC100 must be running firmware version 76 or higher for the PC100 and the IRC2000 panels to function together correctly.

Bosch

It is recommended that the user be familiar with the DS7400Xi panel and has the ability to program PIN codes and parameters into the panel.

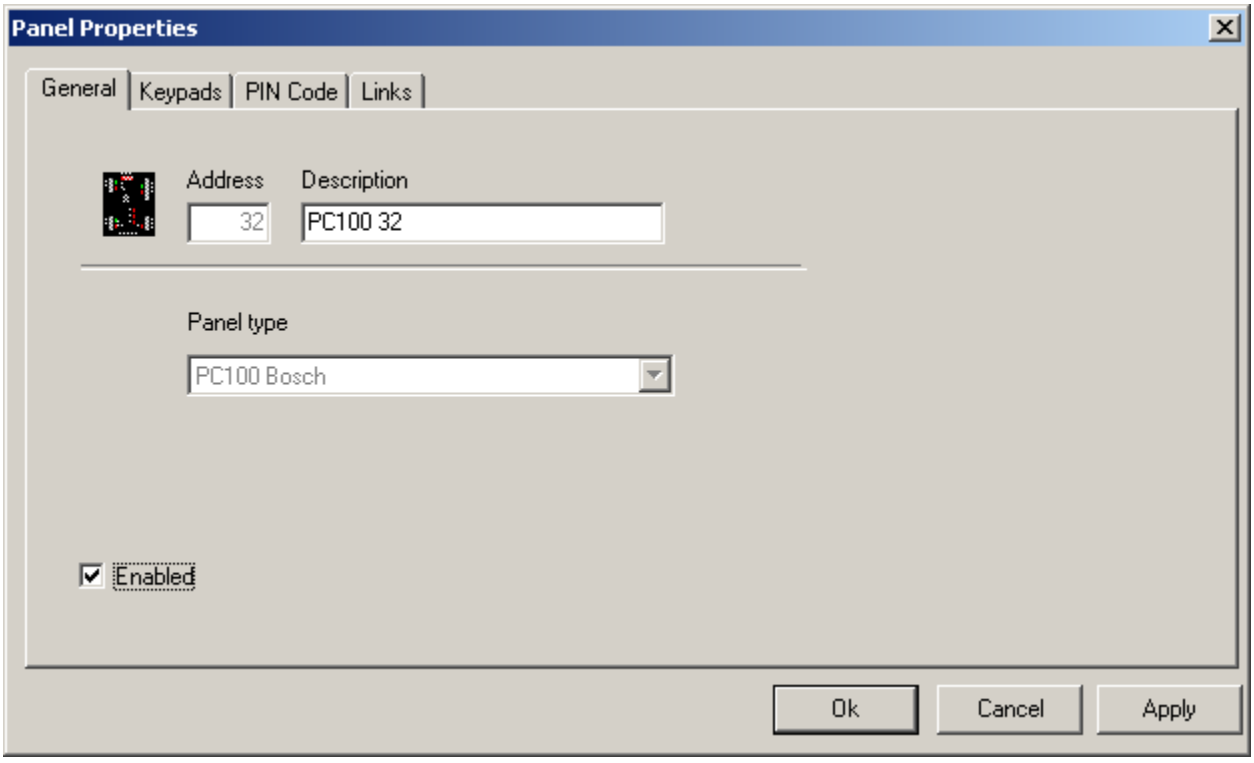
The PC100 interface has been designed to connect the Integra32 network to the DS7400Xi alarm panel through the option or keypad bus. It will emulate a keypad when a link has been provided and report status to the Integra network when included in the list of keypads.

In order for the alarm panel to poll the emulated keypad the keypad assignment for the alarm panel should be programmed. Keypad addresses 1-10 connect to the keypad bus and addresses 11-15 is connected to the option bus.

The PC100 can monitor all keypads on the bus that are listed under panel properties "Keypads".

A Link to an Event will use an emulated keypad to enter a password followed by a command. If the password is not programmed into the alarm panel no operation will take place. Whenever a command is executed the green "Health" LED will turn on. The green "Health" LED will turn off when the alarm panel finishes its poll to the keypad.

General



Address

The address is selected at the time creation and cannot be edited later.

Description

To change the default description simply type over it.

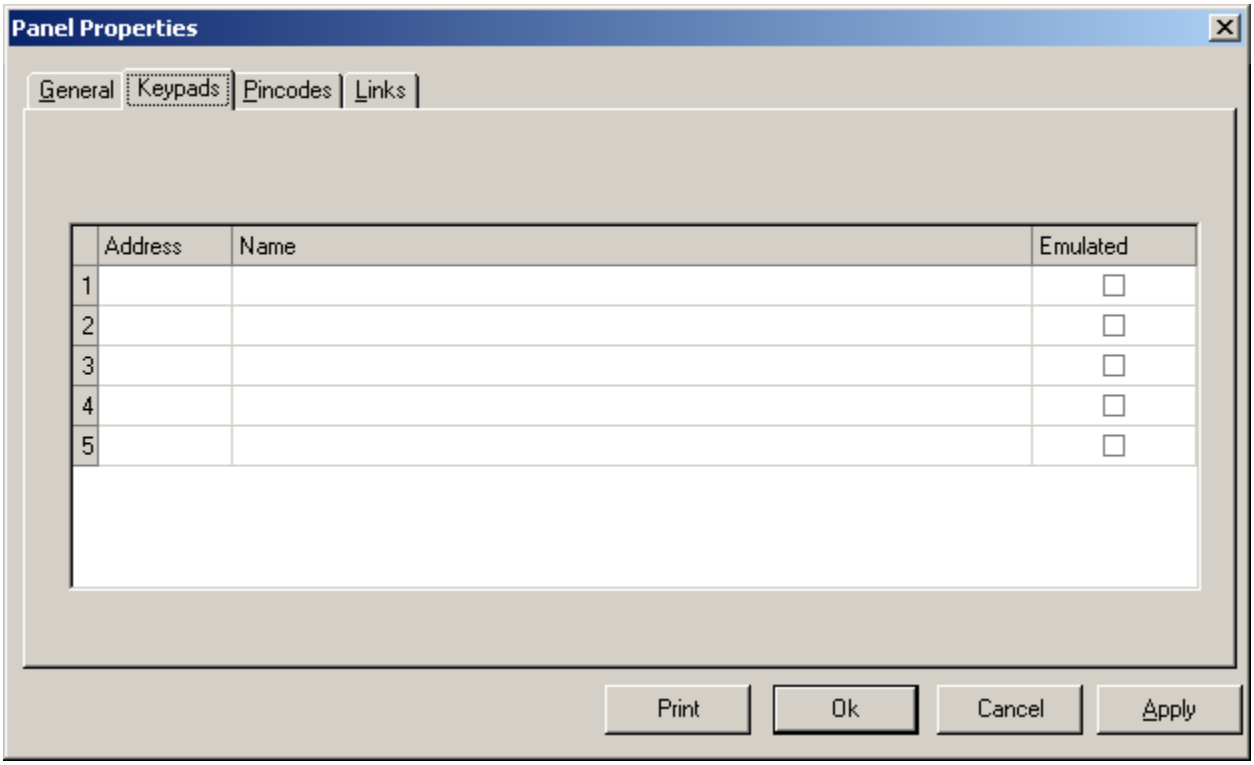
Panel Type

The panel type is chosen when the new panel is added and cannot be edited later.

Enable

If the enable check box is not checked then the panel will not be shown in the status screen. All Access Point, Inputs, and Outputs under that panel will also be disabled. Disabled items are still in the database but are not considered to be part of the system.

Keypads



Address

This is the address of the keypad in the Bosch system (1-15). Only five of the possible fifteen keypads can be selected for use with the PC100.

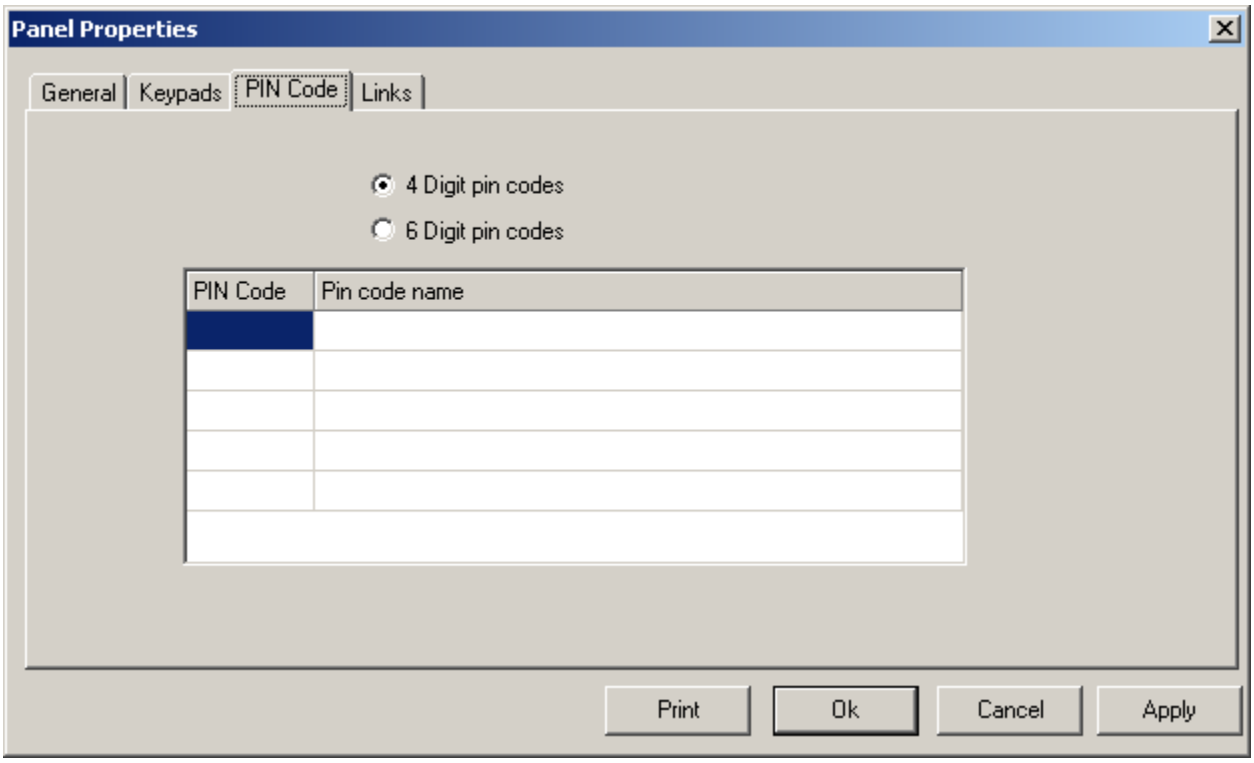
Name

Enter here a description or name of the keypad to be shown in the Integra32™ system.

Emulated

Check this box if the Integra32™ system will be emulating this keypad and leave it unchecked to monitor an existing keypad. Signals from an emulated keypad will be the same as signals from an existing keypad; therefore to the Bosch system there is no difference between an emulated keypad and an existing keypad.

Pin Codes



Select either:

- 4 Digit Pin Codes

  or

- 6 Digit Pin Codes

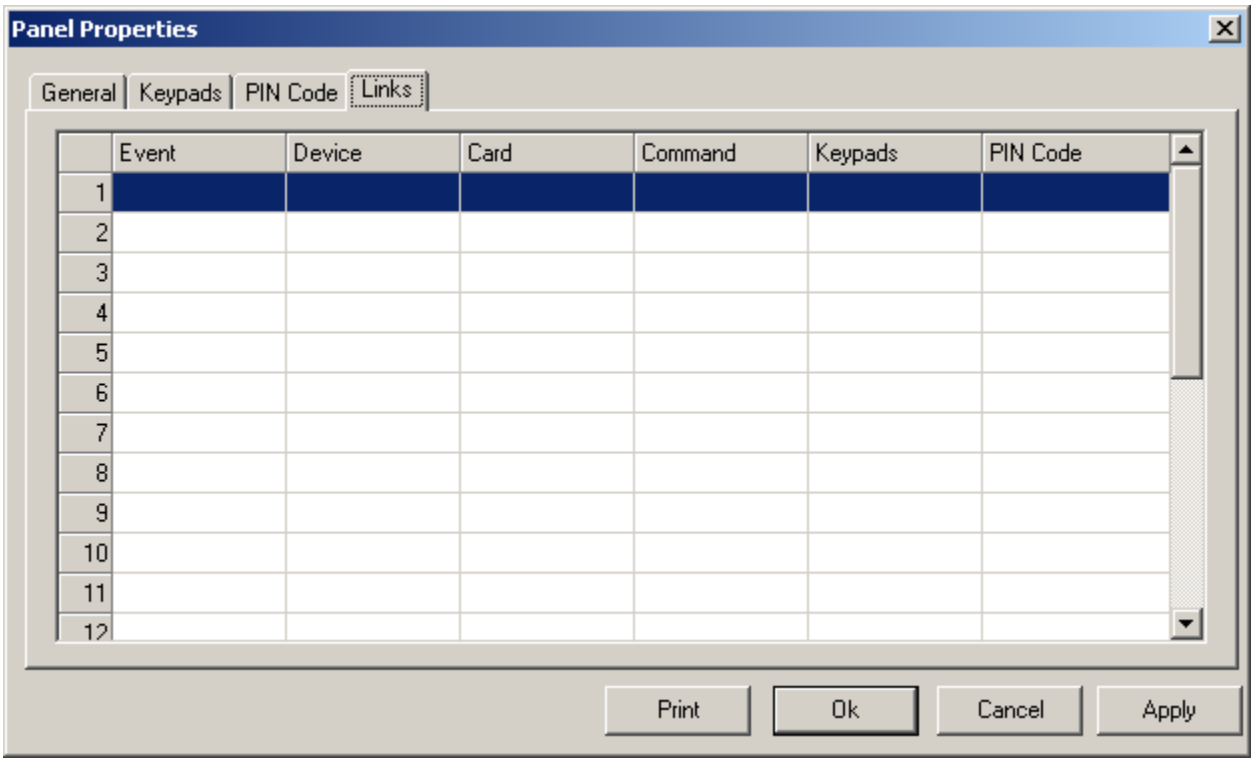
Pin Codes

Enter the four or six digits of each PIN code. These PIN codes must match PIN codes programmed into the Bosch system in order for commands from the emulated keypads to affect the Bosch system. Only five of the possible two hundred PIN codes may be entered here.

Pin Code Name

Enter here a description or name for each PIN code.

Links



Event

Select from a pull down list the triggering event.

Device ID

Choose the appropriate device to execute the selected command from a pull down for the selected event.

Card

Enter the card number (if applicable) that will trigger the selected command when it is associated with the chosen device and selected event (e.g. execute the command when card 1234 is granted access at reader 1).

Command

Select the command to be executed on the chosen keypad from a pull down list (Arm Keypad, Disarm Keypad, or Arm Perimeter).

Keypad

Choose which keypad the command is to be executed on.

Pin Code

Select a valid PIN code. The command will be executed as though this PIN code had been entered.

Summit

The PC100 when made for the Summit application will interface the Electronics Line Gold alarm panel to the IRC2000 access control system.

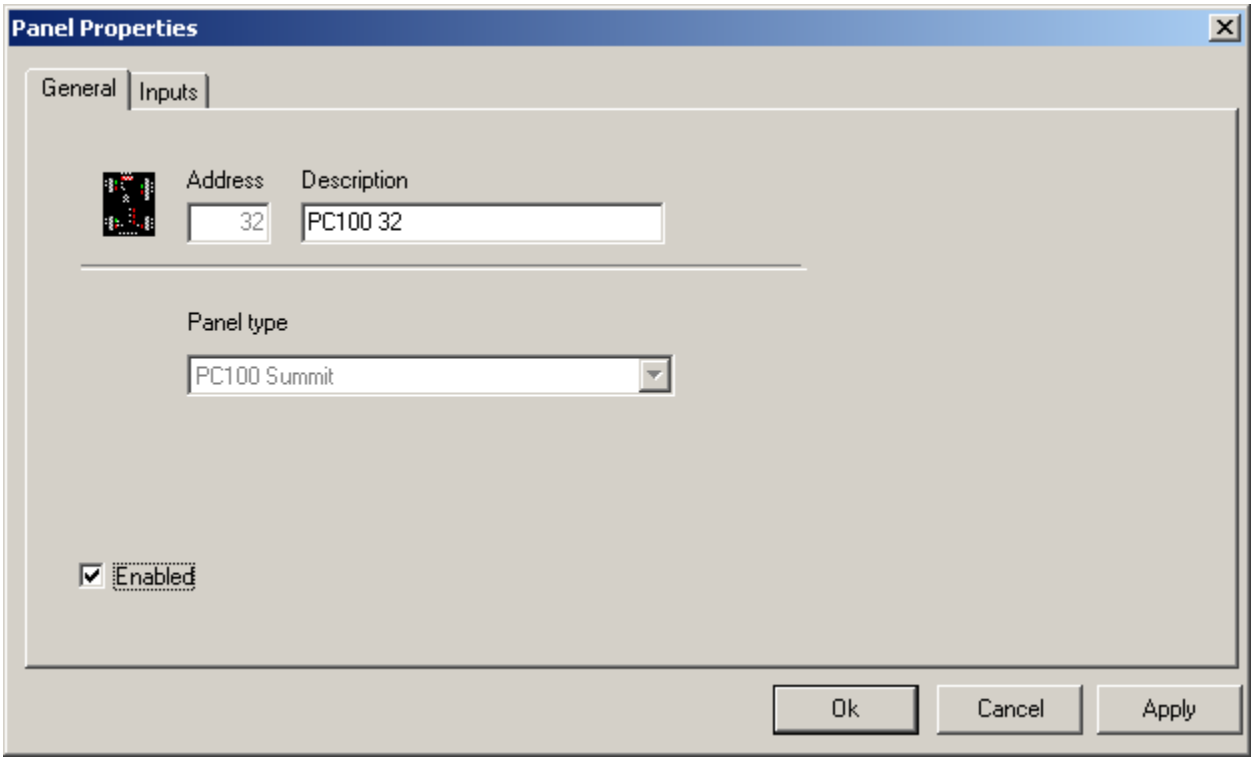
The PC100 comes with three channels of communication all if which are programmed for a baud rate of 9600, eight data bits, and no parity.

The PC100 passes data to and from the host to the IRC network and listens for log messages. In the event where the host is disconnected the PC100 sends request for status from each panel in the network. This prevents log messages from being lost. It takes about 5 seconds for the PC100 to time out and take over the network. When the PC100 has control of the network it will request time and date and keep updating the latest time every 32 polls. When the host comes back on lines all log messages are ignored that are time stamped with a date and time earlier than last recorded. This prevents old messages from triggering false alarms while allowing the host to update its log file. All log messages are passed through the event filter transforming all 128 different log messages into a few events.

All activity is synchronized to the Summit LSCP bus. If the bus is disconnected all activity on the PC100 will halt. The PC100 acts like a zone expander to the Summit panel allowing up to 32 zones. Each zone is mapped to an element in the IRC network. The state of each element in the IRC network will cause a zone to appear open or closed.

The PC100 acts like an IRC panel at address 32 to the host. The host can poll the PC100 to see if it is online, request status, write to memory, and update flash memory.

General



Address

The address is selected at the time creation and cannot be edited later.

Description

To change the default description simply type over it.

Panel Type

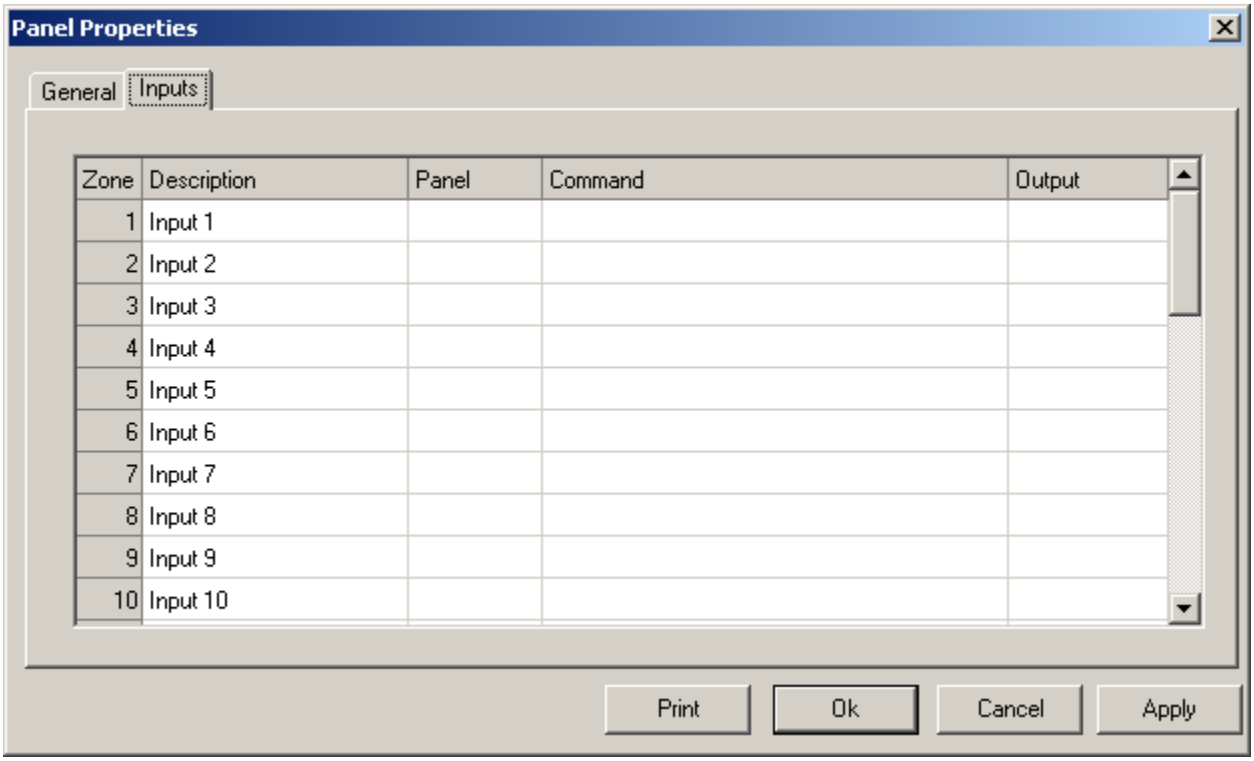
The panel type is chosen when the new panel is added and cannot be edited later.

Enable

If the enable check box is not checked then the panel will not be shown in the status screen. All Access Point, Inputs, and Outputs under that panel will also be disabled. Disabled items are still in the database but are not considered to be part of the system.

Inputs

The inputs of a Summit panel can be affected by the events from Integra32™ access panels. They can follow the access panel's inputs by mimicking them, going into alarm when the access panel's input goes into alarm. Alternatively, they can arm/disarm the Summit panel when access is granted at a reader (the Summit panel's input must be set as an arm/disarm input). On the other hand, they can follow an output on the access panel as if the output was wired to the input.



Zone

There are 32 zones.

Description

The zone name or description can be edited here.

Panel

Designate which panel the input will be affected by.

Command

Choose the function for the input from the pull down list. Does it follow an input or an output, or is it used to arm or disarm the Summit panel.

Output

If the input follows an output designates which output from the pull down list.

Risco Group

It is recommended that the user be familiar with the ("Risco Group") panel and has the ability to program PIN codes and parameters into the panel.

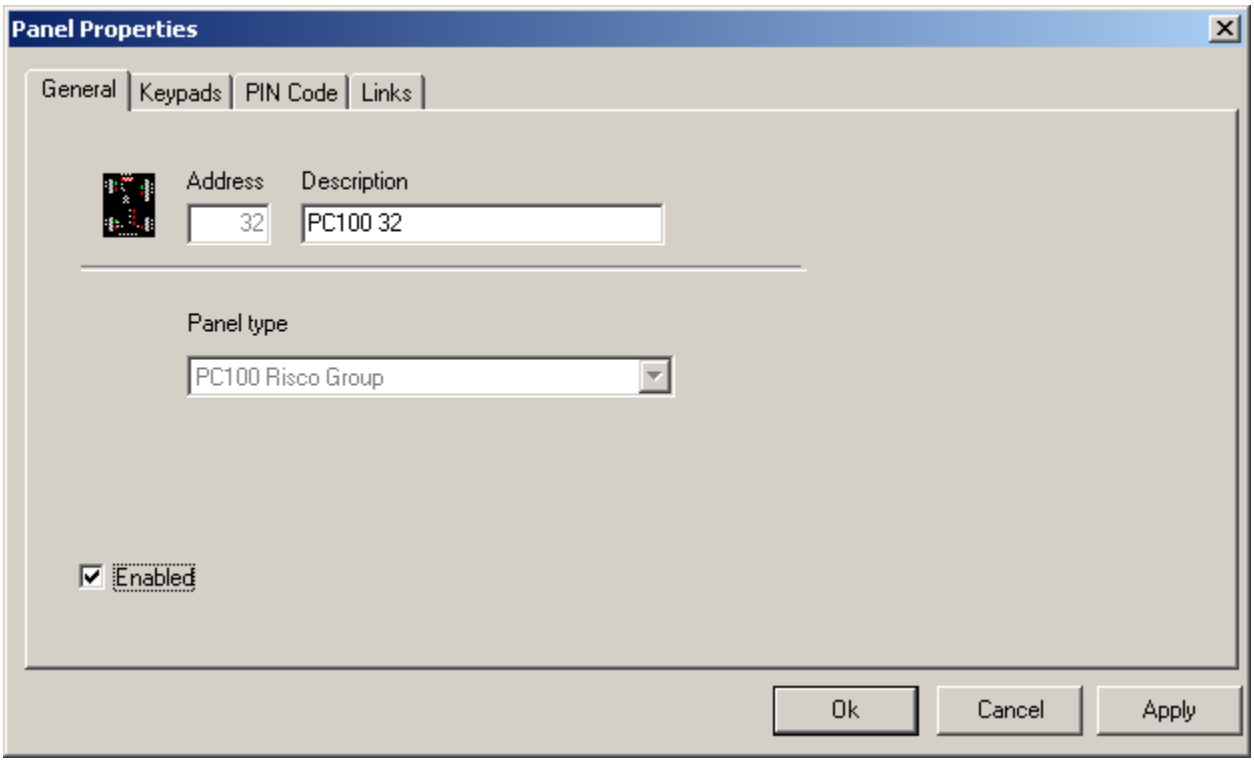
The PC100 interface has been designed to connect the Integra32 network to the ("Risco Group") alarm panel through the option or keypad bus. It will emulate a keypad when a link has been provided and report status to the Integra network when included in the list of keypads.

In order for the alarm panel to poll the emulated keypad the keypad assignment for the alarm panel should be programmed. Keypad addresses 1-10 connect to the keypad bus and addresses 11-15 is connected to the option bus.

The PC100 can monitor all keypads on the bus that are listed under panel properties "Keypads".

A Link to an Event will use an emulated keypad to enter a password followed by a command. If the password is not programmed into the alarm panel no operation will take place. Whenever a command is executed the green "Health" LED will turn on. The green "Health" LED will turn off when the alarm panel finishes its poll to the keypad.

General



Address

The address is selected at the time creation and cannot be edited later.

Description

To change the default description simply type over it.

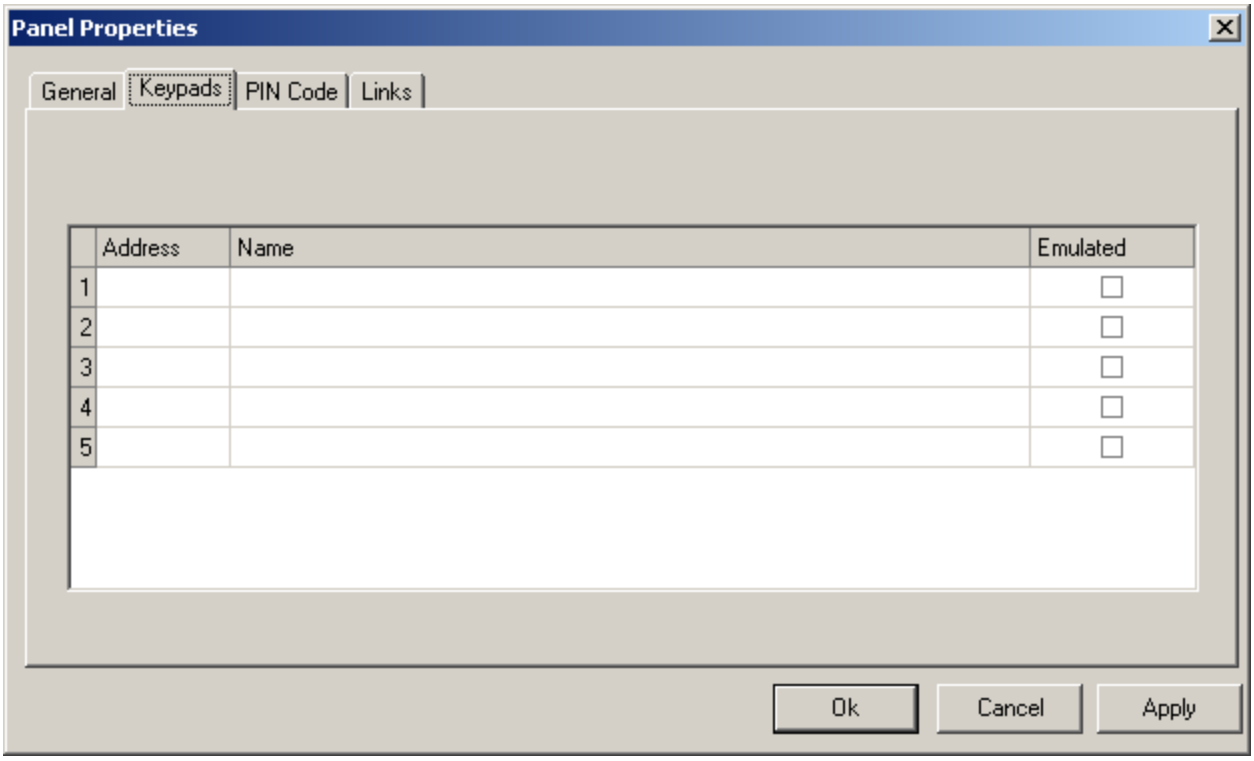
Panel Type

The panel type is chosen when the new panel is added and cannot be edited later.

Enable

If the enable check box is not checked then the panel will not be shown in the status screen. All Access Point, Inputs, and Outputs under that panel will also be disabled. Disabled items are still in the database but are not considered to be part of the system.

Keypads



Address

This is the address of the keypad in the Risco Group system (#?).

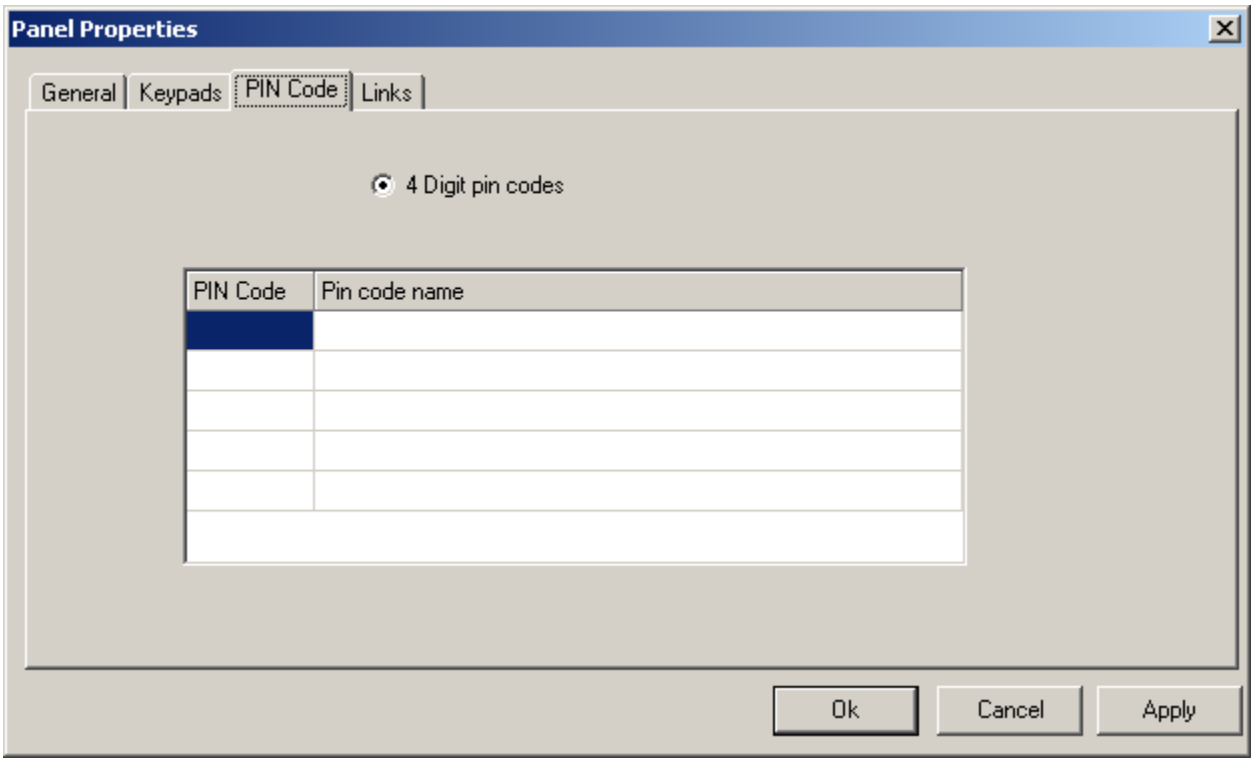
Name

Enter here a description or name of the keypad to be shown in the Integra32™ system.

Emulated

Check this box if the Integra32™ system will be emulating this keypad and leave it unchecked to monitor an existing keypad. Signals from an emulated keypad will be the same as signals from an existing keypad; therefore to the Risco Group system there is no difference between an emulated keypad and an existing keypad.

PIN Code



⊙ 4 Digit Pin Codes

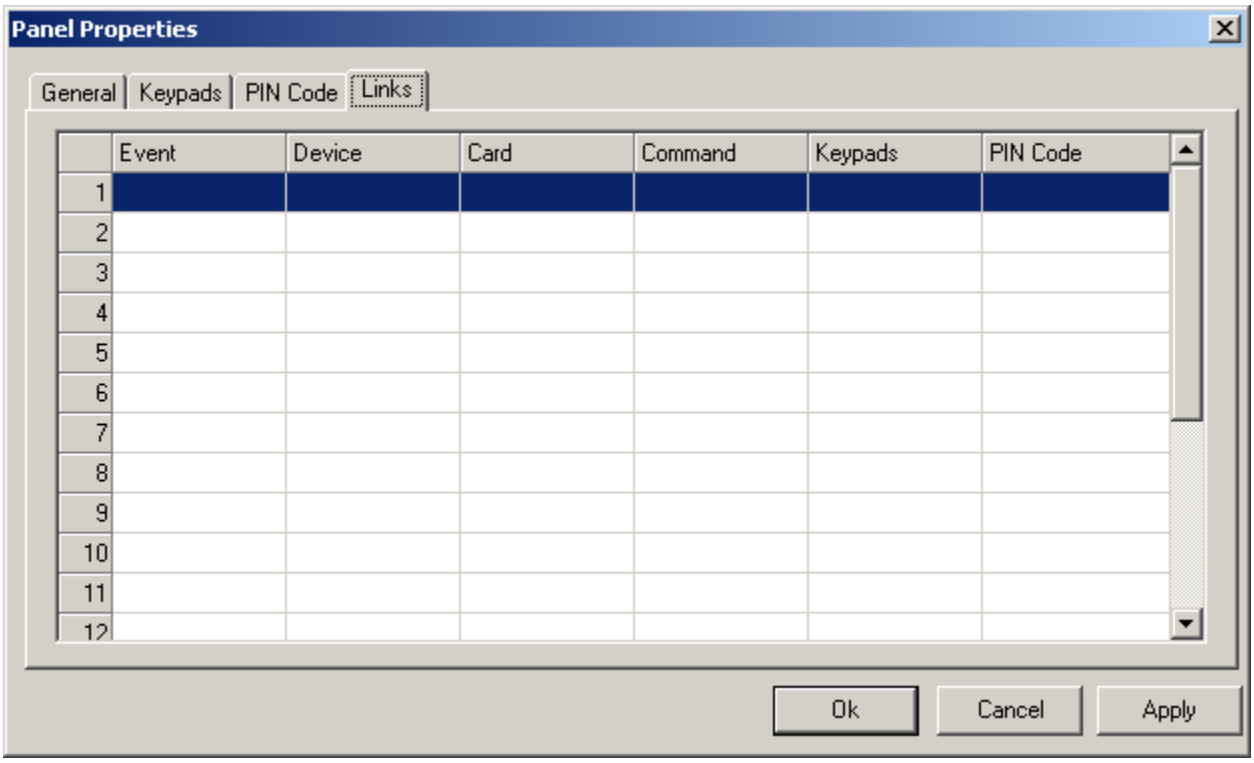
Pin Codes

Enter the four digits of each PIN code. These PIN codes must match PIN codes programmed into the Risco Group system in order for commands from the emulated keypads to affect the Risco Group system. Only five of the possible two hundred PIN codes may be entered here.

Pin Code Name

Enter here a description or name for each PIN code.

Links



Event

Select from a pull down list the triggering event.

Device ID

Choose the appropriate device to execute the selected command from a pull down for the selected event.

Card

Enter the card number (if applicable) that will trigger the selected command when it is associated with the chosen device and selected event (e.g. execute the command when card 1234 is granted access at reader 1).

Command

Select the command to be executed on the chosen keypad from a pull down list (Arm Keypad, Disarm Keypad, or Arm Perimeter).

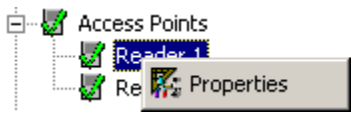
Keypad

Choose which keypad the command is to be executed on.

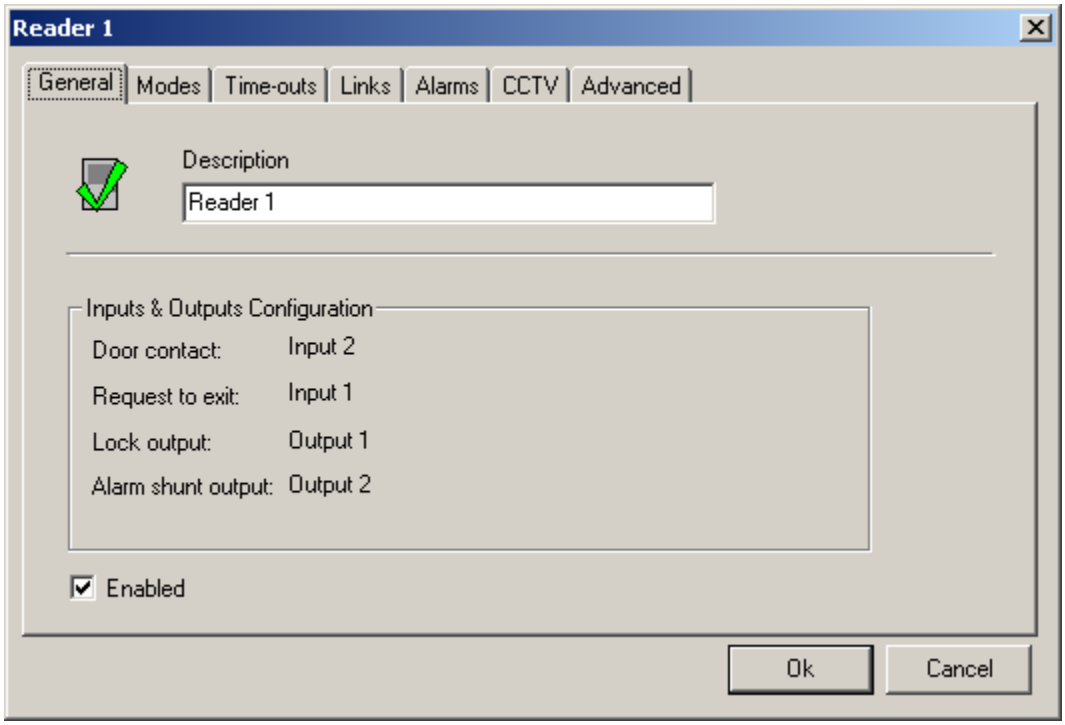
Pin Code

Select a valid PIN code. The command will be executed as though this PIN code had been entered.

Access Points



General



Description

To change the default description simply type over it.

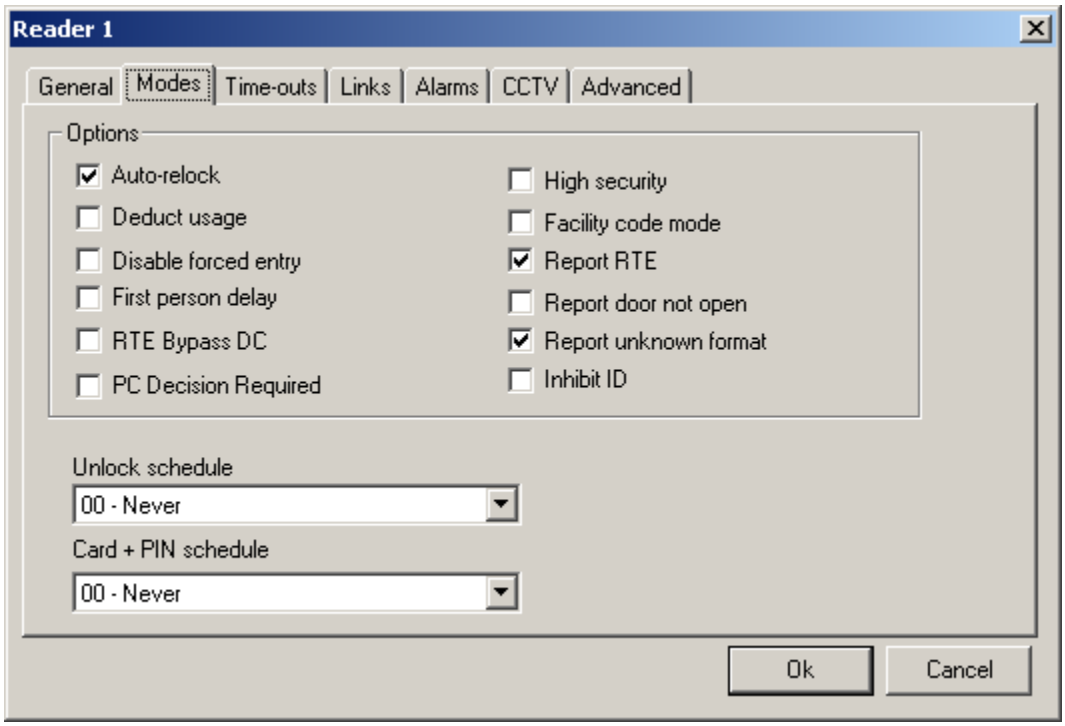
Input & Output Configuration

This section of the tab tells you which inputs and outputs are assigned to the access point.

Enable

If the enable check box is not checked then the access point will not be shown in the status screen and will not be considered as part of the system.

Modes



Auto-Relock

After a grant access the door locks again at the end of the unlock time. With auto-relock checked if the door closes before the unlock time expires, then the door will lock when the door closes and won't wait until the timer expires.

Deduct Usage

Readers selected to deduct usage will reduce the usage count of cards granted access if the cards' usage count is less than 255. Card with a usage count of zero will not be granted access. Usage count works per panel if the system is run offline. Systems that are run online will have the usage count of a cardholder updated in all panels when any reader reduces that cardholder's count.

✎ **This feature doesn't work in conjunction with *PC Decision Required*. *PC Decision Required* will override *Deduct Usage*.**

Disable Forced Entry

If Forced Entry is disabled then opening the door without an access granted will not cause a Forced Entry alarm but instead will start the access granted sequence. This is generally used on a door with a mechanical egress and no request to exit device.

First Person Delay

Access points with lock/unlock schedules will lock and unlock according to the schedule. If First Person Delay is selected the door will remain locked until the first card is granted access after the start of the schedule.

RTE Bypass DC

This feature is used with the doors having mechanical egress. The Request to Exit device will bypass the door contact but will not unlock the door. The door can be opened without causing an alarm since the contact is bypassed.

PC Decision Required

Selecting *PC Decision Required* takes the decision to grant access away from the panel. If the panel would normally grant access, it wouldn't. Instead it simply sends a message to the PC "*Access Requested"*. An operator at the PC can then decide to grant access or not. Other software functions can also use this feature (*e.g. global Antipassback*).

✎ **This feature doesn't work in conjunction with *Deduct Usage*. *PC Decision Required* will override *Deduct Usage*.**

High Security

Only cards with High Security privilege will be granted access at access points in High Security mode.

Facility Code Mode

Access points in Facility Code Mode will grant access based upon the card's facility code and not on the card's card number. Cards not entered into the system that have the correct facility code will be granted access.

Report RTE

Access granted by a request to exit device will report that event, if this feature is checked.

Report Door Not Open

The fact that a door was not opened after access was granted at that door can be reported if this feature is checked.

Report Unknown Format

An Unknown Format message indicates that the data received does not correspond to any of the card formats useable by the IRC-2000. This message can be turned off if it is not required.

Inhibit ID

The cardholder name and card number will be blocked for access granted messages if this feature is checked. 'Access granted RTE' message will be shown in place of 'Access granted by card'. This feature is not applicable for **Card + PIN** schedule.

Unlock Schedule

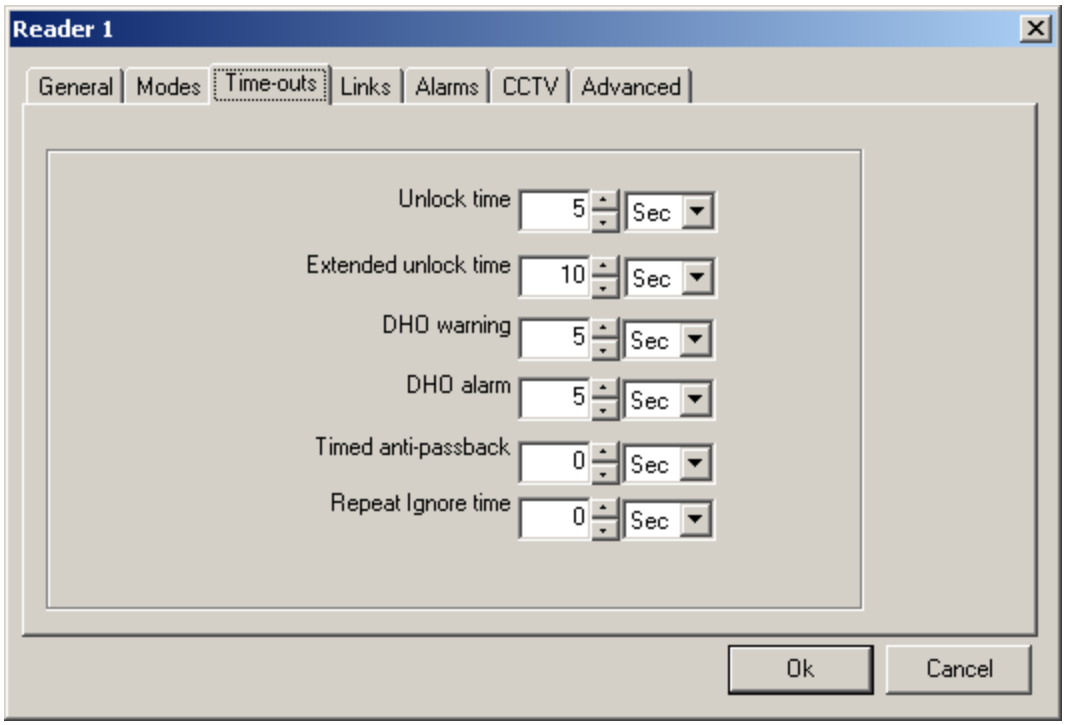
Select a schedule when unlocking and locking of this access point is required.

Card + PIN Schedule

Select a schedule when both Card and PIN are required. When this schedule is off only a Card is needed for access to be granted.

Time-Outs

Timers can be set from 0-127 seconds or minutes. Setting a timer to zero will disable it.



Unlock Time

This is the time the Door Unlock output is turned on for.

Extended Unlock Time

For the Cards given the Extended Unlock Time privilege the Door Unlock output will turn on for this length of time instead of the regular Unlock Time.

DHO Warning

If a door is still open when the Lock Time expires, the Door Held Open Warning timer will start. When the Door Held Open Warning time expires the Access Point will go into Door Held Open Warning (posting DHO Warning message and pulsing the reader's buzzer).

DHO Alarm

If a door is still open when the Door Held Open Warning time expires, the Door Held Open Alarm timer will start. When the Door Held Open Alarm time expires the Access Point will go into Door Held Open Alarm (posting DHO Alarm message and turning on the reader's buzzer continuously). Since the DHO Alarm timer starts when the DHO Warning timer expires, if the DHO Warning time is set to zero then the DHO Alarm timer won't be started.

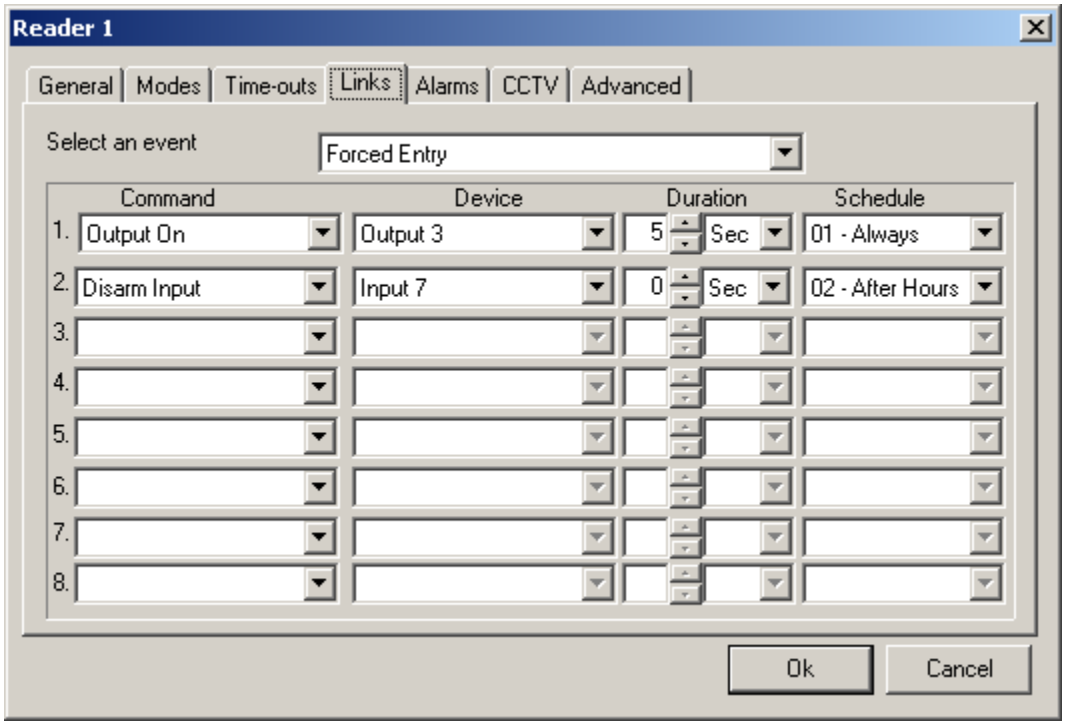
Timed Antipassback

Set the amount of time for Timed Antipassback here. Timed Antipassback will reset at the end of the programmed time allowing the cardholder to be granted access into an area they are already logged into. If a cardholder tries to re-enter an area before the timer expires they will cause an antipassback violation.

Repeat Ignore Time

Set the amount of time after a card is read until that card can be use again at that door. After the card is read, that card will be ignored for the set amount of time. Other cards can be used and each will be subject to the ignore time individually.

Links

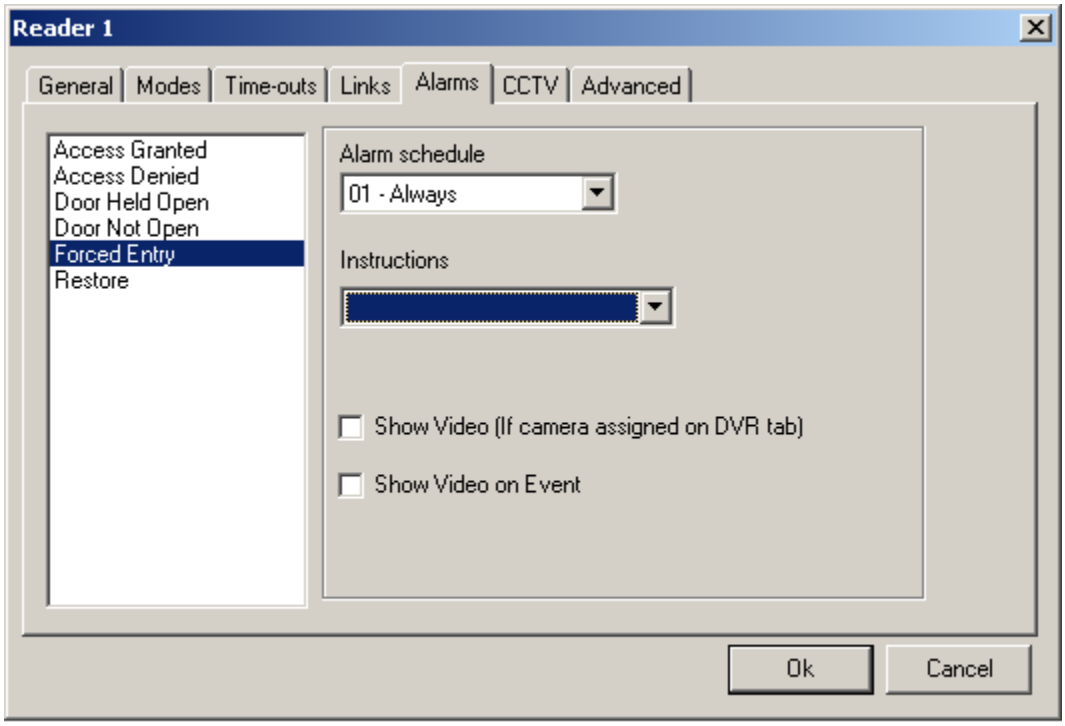


- First select an event.
  - The selectable events are Access Granted, Access Denied, Door Locked, Door unlocked, Door Held Open, Door Not Open, Forced Entry, Restore, High Security On, High Security Off, 3* Links, and 5* Links (3* Links and 5* Links indicate either three or five consecutive Access Granteds to execute the link), and Access Granted RTE.

- Then select up to eight commands to be executed with that event.
  - The command selection list includes; arming or disarming an input, turning on or off an output, locking or unlocking an access point, setting High Security mode on or off for an access point, and turning Disable Forced Entry on or off.
- After you have selected a command an appropriate device needs to be selected (*input, output, or access point*).
- Choose the duration of the command (*0-127 seconds or 0-126 minutes*).
  - Not all commands can be timed. *High Security* on and off, and *Disable Forced Entry* on and off cannot be timed.
- A schedule can also be selected for each command (*the command will only be executed when the schedule is on*).

The example above has the Output 3 being turned on for five seconds and Input 7 will be disarmed when there is a forced entry at Reader 1 (but only during the specified schedule associated with each point).

Alarms



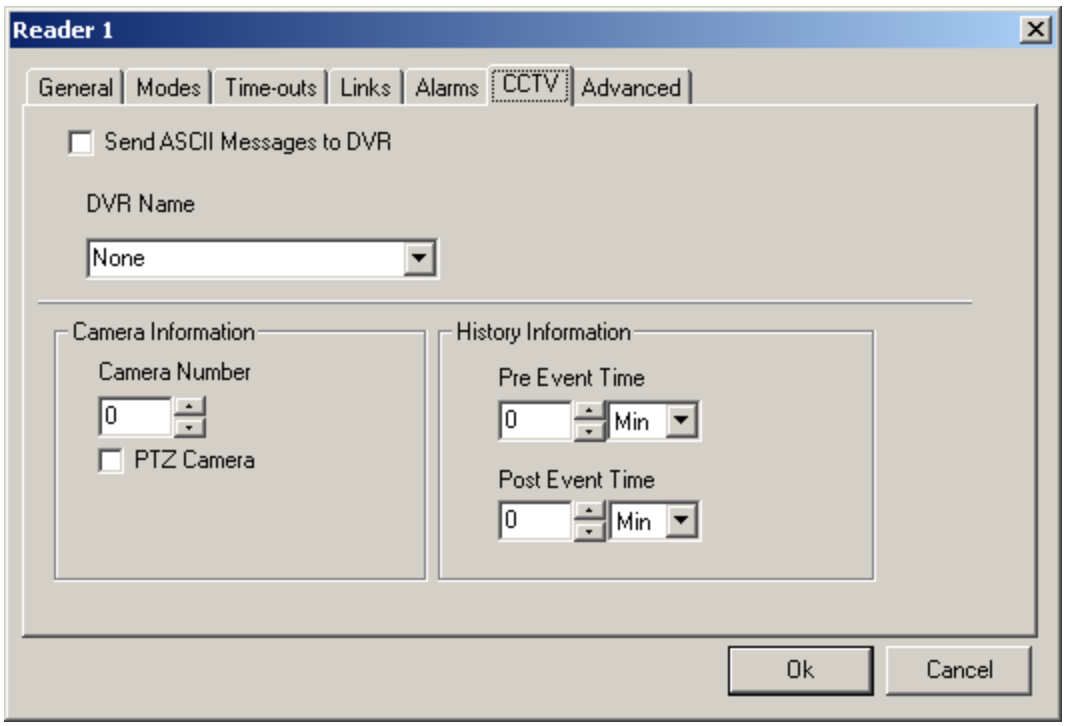
- First select an event from list on the left.
  - The alarm will occur when the message appears in the log screen.
- Then select an *Alarm Schedule*. (*Causes an alarm when*?)
- Then you can select (*if required*) an instruction message for the alarm. (*Message creation is described earlier*.)

- ☑ Show Video (If camera assigned on DVR tab): Check this box to have the DVR show the camera configured on the CCTV tab for this access point on the configured Alarm.
- ☑ Show Video on Events: Check this box to have the DVR show the camera configured on the CCTV tab for this access point on the configured message (Alarm is not required).

CCTV[16]

This tab is only available if the CCTV module has been installed.

The information in this tab is only used to interface with a DVR. There are two ways that this interface can be accomplished.



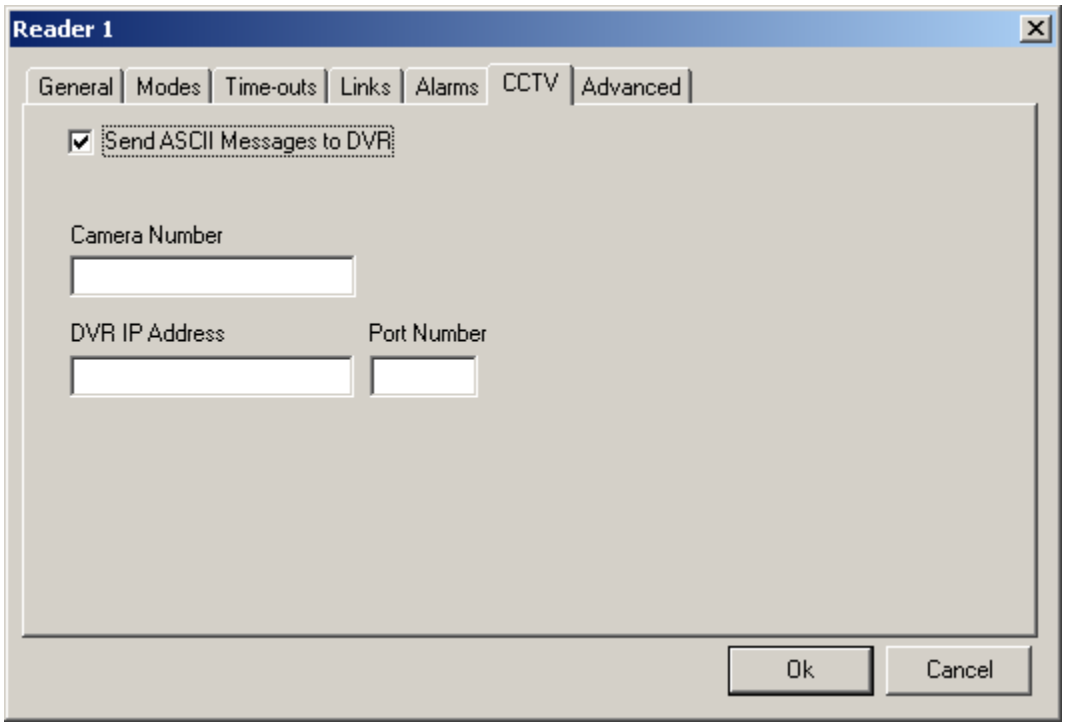
One way the interface can be used is to associate the reader with a specific DVR. DVRs are set up in the *Database Screen* under DVR.

- First select a DVR for the pull down list under *DVR Name*.
- Next configure the *Camera Information*. Select a camera number, indicate whether it's a PTZ camera or not, and if it is enter a preset number if applicable.
- Then set the *History Information*. Set the *Pre Event Time*, and the *Post Event Time*. These times set playback start time (how much time before the event time) and the playback end time (how long to continue the playback after the event

[16] This selection is only available if the optional license for the DVR Software has been purchased and installed.

time). This configuration is used by the History Reports DVR tab to playback video associated with a logged event.

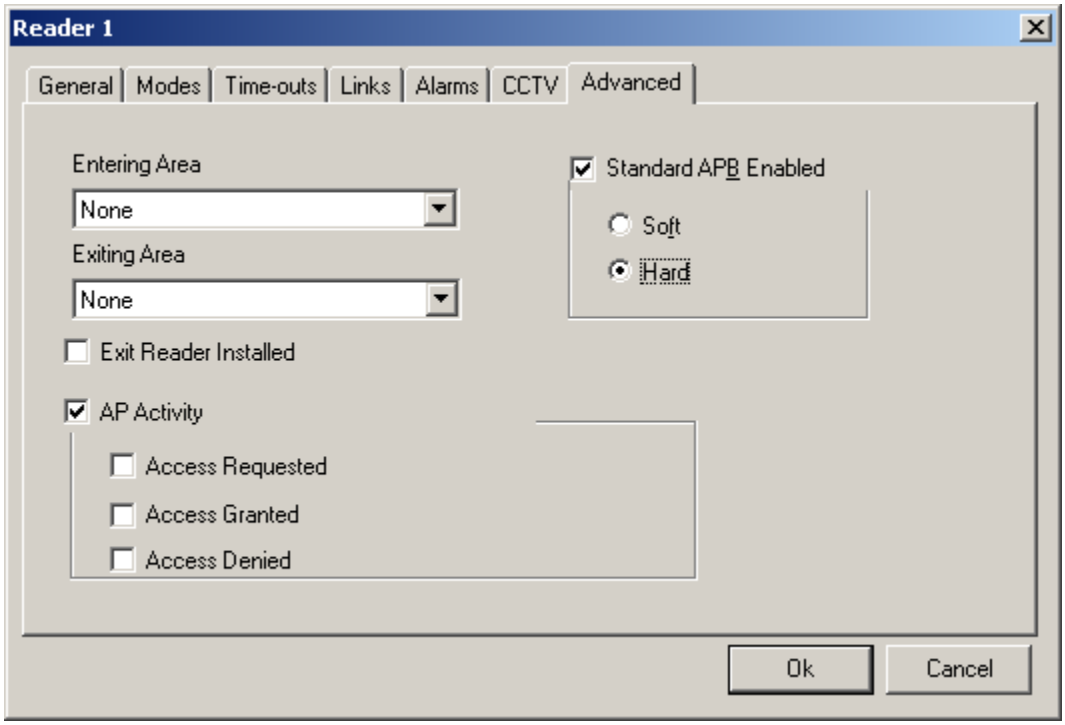
The second way is by using ASCII messages.



☑ Send ASCII Message to DVR

- First select the camera number you want to display from DVR.
- Then enter the DVR's IP address and Port Number associated with the camera you selected as you could be using more than one DVR (this configuration is used by the History Reports DVR tab to playback video associated with a logged event).

Advanced



Standard APB Enabled

The check box is used to turn on antipassback. Soft antipassback will still grant access even though APB has been violated, hard APB will not.

Global/Local Antipassback

For Global Antipassback[17] to work the Integra32™ system must be online, and *PC Decision Required* must be turned on in the *Modes* tab of the Reader Properties' window for all of the appropriate readers, otherwise the panel will default to Local Antipassback[18] (*within an IRC-2000*). Global Antipassback allows a cardholder's area to be reset/cleared, meaning they are not logged into any area. With Local Antipassback the cardholder is either 'In' or 'Out' (*never neither, always one or the other*). Local Antipassback may be used with or without the Exit Reader Interface.

If the Exit Reader Interface is not used when Local Antipassback is configured, then either the 'A' side or the 'B' side reader port (*not both*) needs to have its TAM terminal grounded. The side with the grounded TAM terminal will be the 'Out' reader and the side without will be the 'In' reader.

[17] Antipassback tracked across multiple IRC-2000s is called *Global Antipassback*.

[18] Antipassback tracked on one side of a panel (*IRC-2000*) is called *Local Antipassback*.

Entering Area & Exiting Area

An Entering Area must be selected for APB to work. Selecting only an Entering Area will setup Reader APB. In Reader APB the Entering Area is compared to the cardholder's current location. If they match there is an APB violation. By adding an Exiting Area you setup Area APB. Area APB not only check that the area the cardholder is entering isn't the area they are in, but also verifies that the area they are exiting is the area they currently are in, providing a higher level of APB.

APB Access Points work well with Exit Reader Interfaces. The 'In' reader uses the configuration of Entering Area and Exiting Area as programmed while the 'Out' reader uses the inverse. (The 'Out' reader gets its Entering Area from the data programmed into Exiting Area and vice versa.)

Out Reader Install

Selection of this option will configure the system to allow separate Global links for the 'In' reader as for the 'Out' reader.

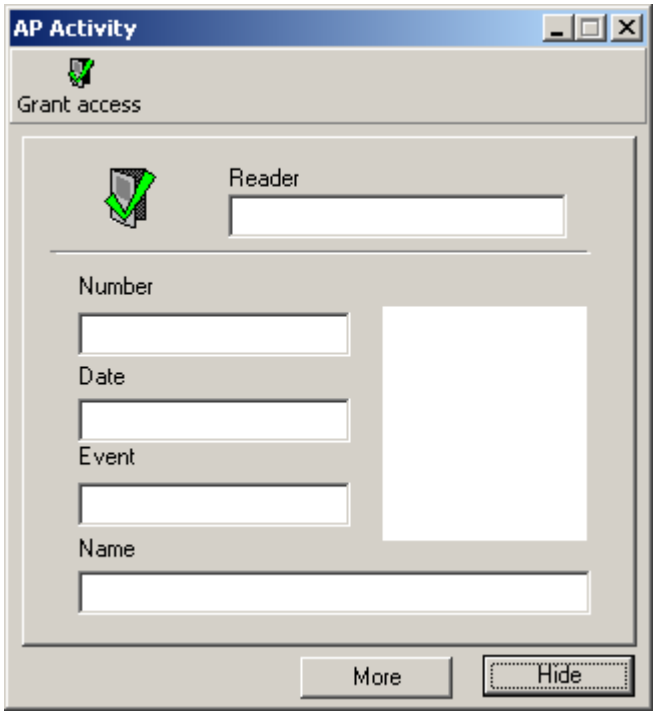
The Exit Reader Interface module is used to connect two readers to a single reader port providing both 'In' and 'Out' readers.

To use the Exit Reader Interface module the IRC2000 must be running firmware 100 or higher.

Access Point Activity

By checking this box you enable the automatic displaying of the Access Point Activity window when the selected event(*s*) occur at the access point. Often this is used with a CCTV system for video verification of access.

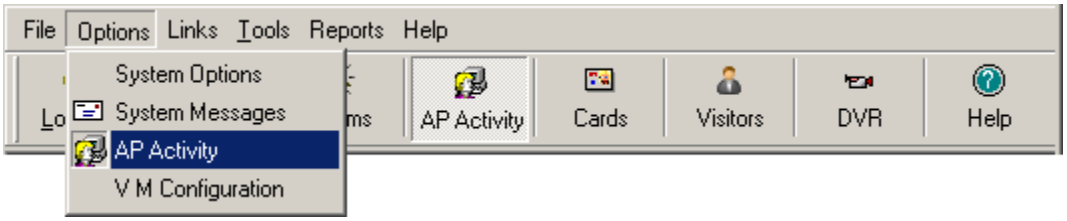
Multiple readers may be select to be displayed with this window. Only the last event is displayed though, all previous displays are deleted.



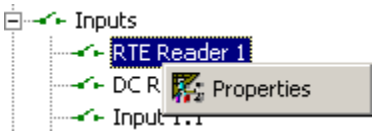
Grant Access

Grant access will grant access at the reader currently shown in the *Reader* box of the *Access Point Activity* window.

Note: The above window is automatically displayed only if *Access Point Activity* is turned on, either from the *Options* menu or on the main screen toolbar.



Inputs



General

From *General* tab the user can change the description of the input. The *Type* of input is also chosen here.

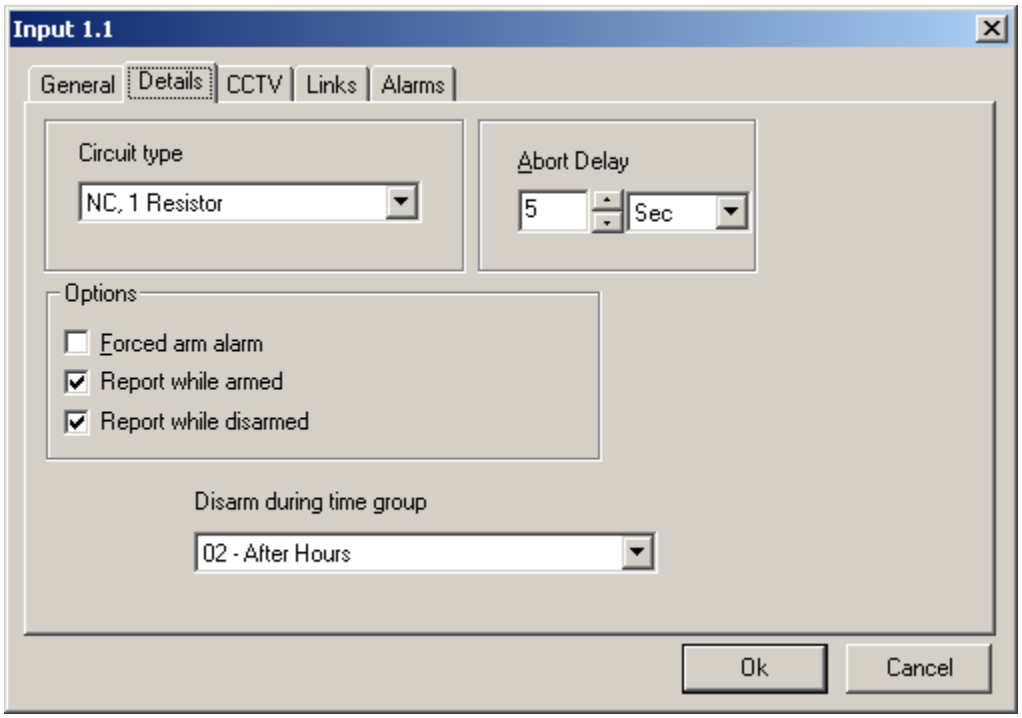
- The input type can be:
  - General Purpose
  - RTE for Reader A
  - RTE for Reader B
  - Door Contact for Reader A
  - Door Contact for Reader B

Details

Select the *Circuit type* and *Abort Delay* under the *Details* tab.

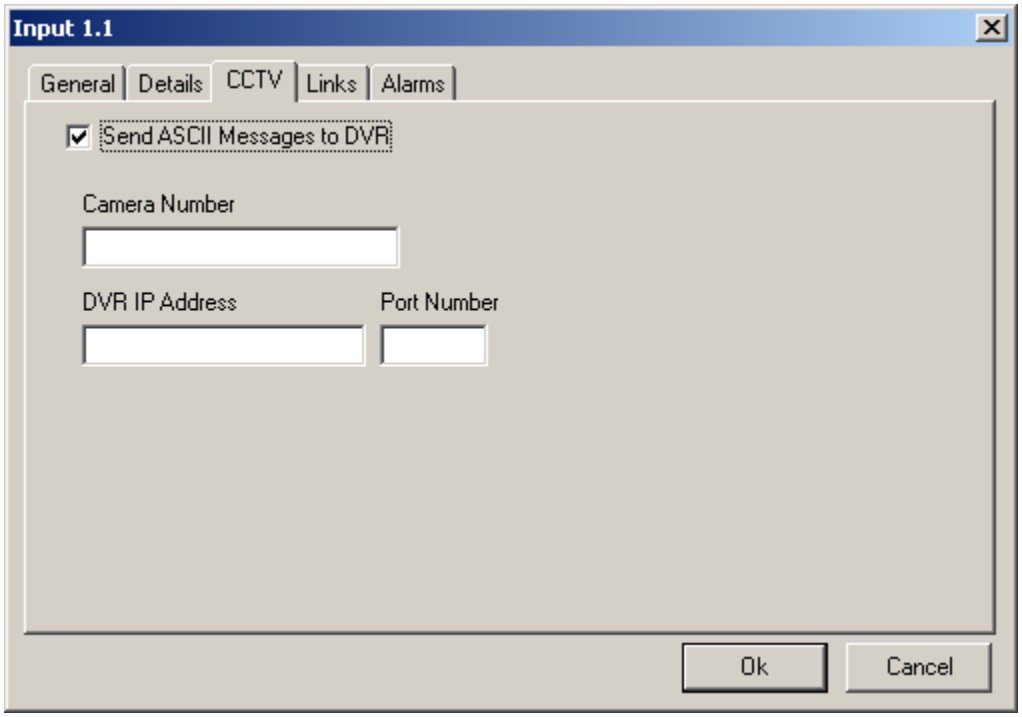
- Inputs can be:
  - Normally Open or Normally Closed
  - One resister, Two resister, or No resister
- Abort Delay is set in second/minutes (*maximum 127 minutes*).
  - The input must be tripped for this amount of time to cause an alarm. If the input is cleared before the time expires then there won't be an alarm.

For *General Purpose* inputs additional programming is required under the Details tab.



- Reporting or Non-reporting. (*Are messages from this input to be displayed on the Log Screen and logged*?)
- Forced Arm Alarm or Not Forced Arm Alarm. (*Forced Arm Alarm will force an input into alarm if it is armed while it is abnormal*.)
- Disarm during Time Group. (*Disarm the input during a schedule*.)

CCTV[19]



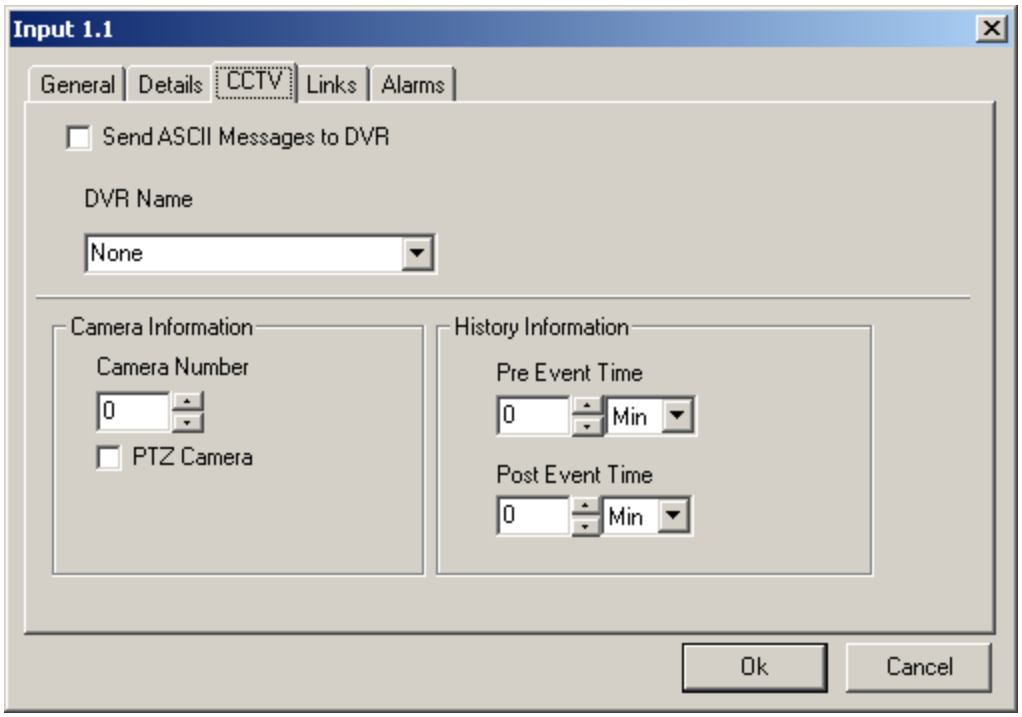
This tab is only available if the CCTV module has been installed.

The information in this tab is only used to interface with a DVR. There are two ways that this interface can be accomplished. The first is by using ASCII messages.

☑ Send ASCII Message to DVR

- First select the camera number you want to display from DVR.
- Then enter the DVR's IP address and Port Number associated with the camera you selected as you could be using more than one DVR (this configuration is used by the History Reports DVR tab to playback video associated with a logged event).

[19] This selection is only available if the optional license for the DVR Software has been purchased and installed.



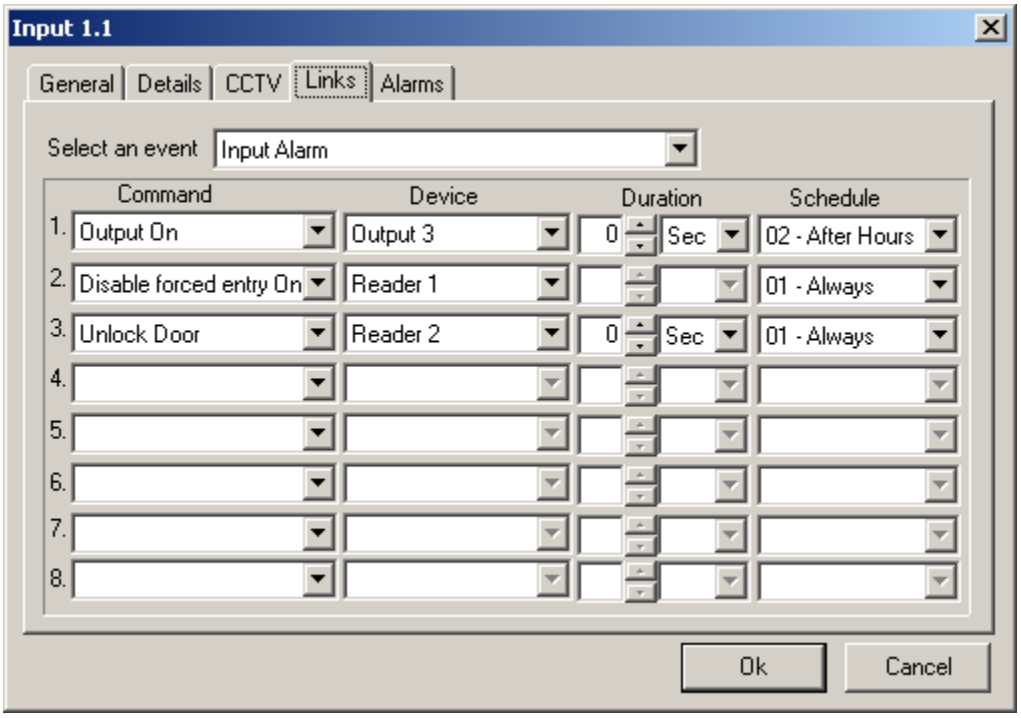
The second way the interface can be used is to associate with a specific DVR. DVR are set up in the *Database Screen* under DVR.

- First select a DVR for the pull down list under *DVR Name*.
- Next configure the *Camera Information*. Select a camera number, indicate whether it's a PTZ camera or not, and if it is enter a preset number if applicable.
- Then set the *History Information*. Set the *Pre Event Time*, and the *Post Event Time*. These times set playback start time (how much time before the event time) and the playback end time (how long to continue the playback after the event time).

This configuration is used by the History Reports DVR tab to playback video associated with a logged event.

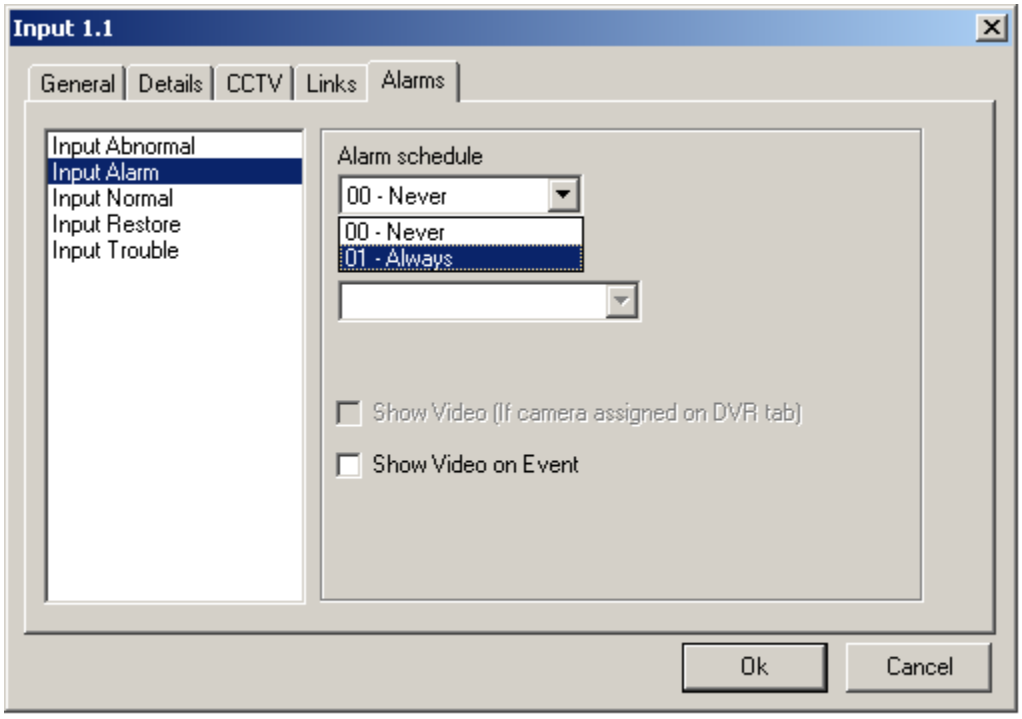
Links and *Alarms* tabs are available only for general-purpose inputs.

Links



- First select an event.
  - Selectable events are Input Abnormal, Input alarm, Input Normal, Input Restore, and Input Trouble.
- Then select up to eight commands to be executed with that event.
  - The command selection list includes; arming or disarming an input, turning on or off an output, locking or unlocking an access point, setting High Security mode on or off for an access point, and turning Disable Forced Entry on or off.
- After you have selected a command an appropriate device needs to be selected (*input, output, or access point*).
- Choose the duration of the command (*0-127 seconds or 0-126 minutes*).
  - Not all commands can be timed. *High Security* on and off, and *Disable Forced Entry* on and off cannot be timed.
- A schedule can also be selected for each command (*the command will only be executed when the schedule is on*).

Alarms

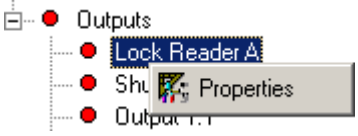


- First select an event from the list on the left.
  - The alarm will occur when the message appears in the log screen.
- Then select an *Alarm Schedule*. (*Causes an alarm when*?)
- Then you can select (*if required*) an instruction message for the alarm. (*Message creation is described earlier*.)

☑ Show Video (If camera assigned on DVR tab): Check this box to have the DVR show the camera configured on the DVR tab for this input on configured Alarm

☑ Show Video on Event: Check this box to have the DVR show the camera configured on the DVR tab for this input on configured event.

Outputs

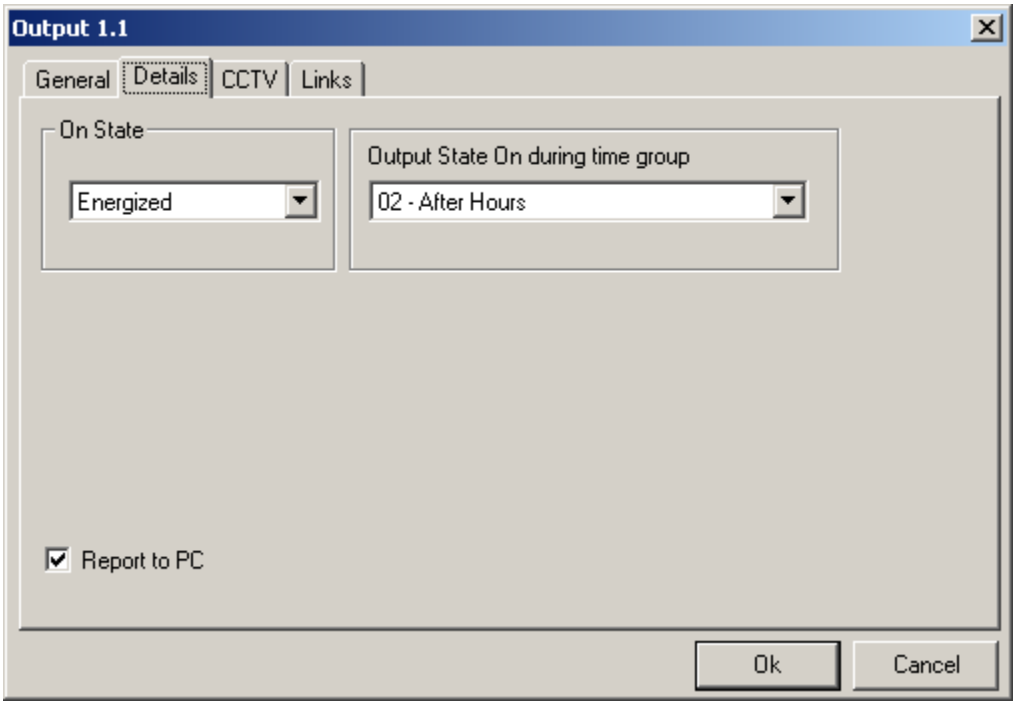


General

The *Description* and *Type* of the output can be changed/programmed in the *General* tab.

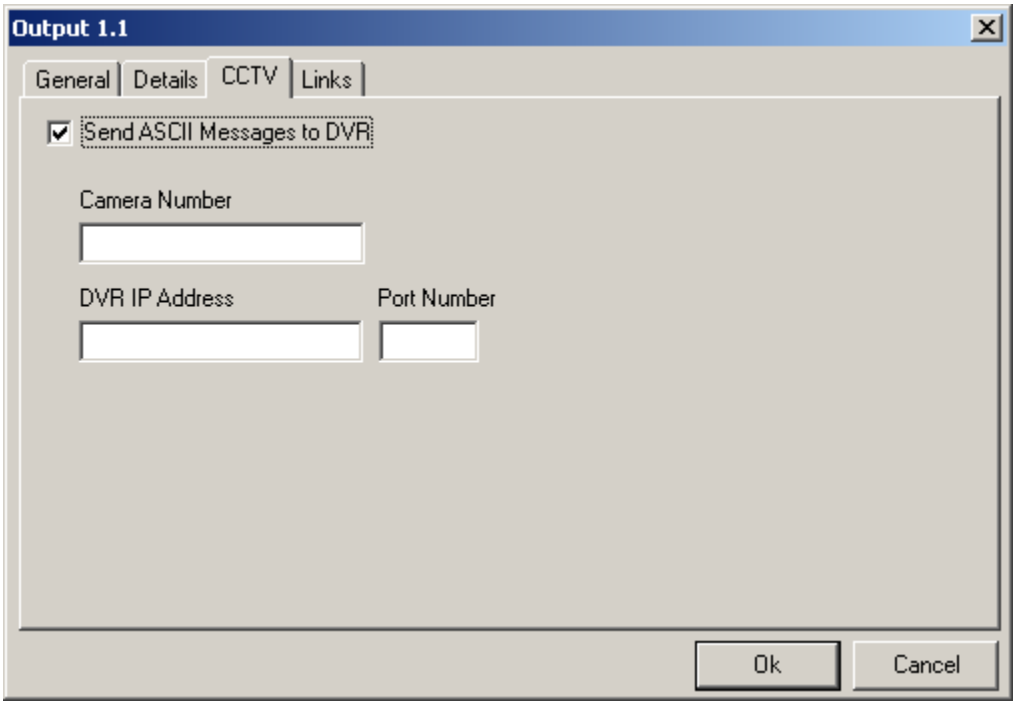
- The output type can be:
  - General Purpose
  - Lock for Reader A
  - Lock for Reader B
  - Handicap for Reader A
  - Handicap for Reader B
  - Alarm Shunt A
  - Alarm Shunt B
  - Modem Power

Details



Choose *Energized/De-energized On State* and select a schedule for *Output State On During Time Group* from the *Details* tab. Also select the option of *Report to PC*, if it is needed. *Output State On During Time Group* and *Report to PC* are programmable for general-purpose outputs only.

CCTV[20]



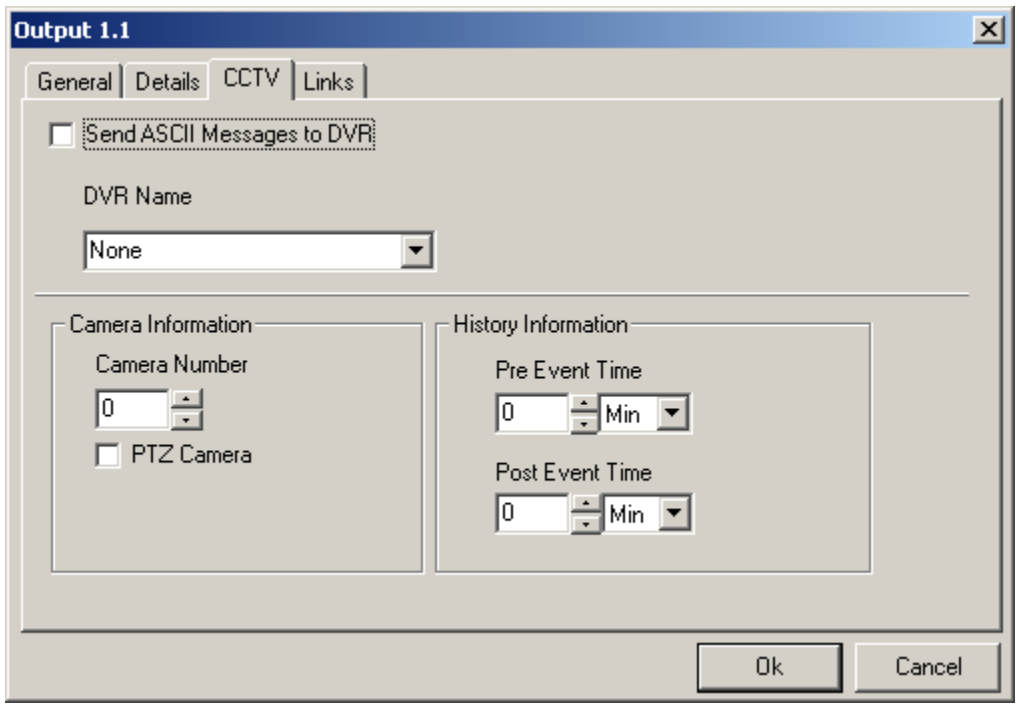
This tab is only available if the CCTV module has been installed.

The information in this tab is only used to interface with a DVR. There are two ways that this interface can be accomplished. The first is by using ASCII messages.

☑ Send ASCII Message to DVR

- First select the camera number you want to display from DVR.
- Then enter the DVR's IP address and Port Number associated with the camera you selected as you could be using more than one DVR (this configuration is used by the History Reports DVR tab to playback video associated with a logged event).

[20] This selection is only available if the optional license for the DVR Software has been purchased and installed.



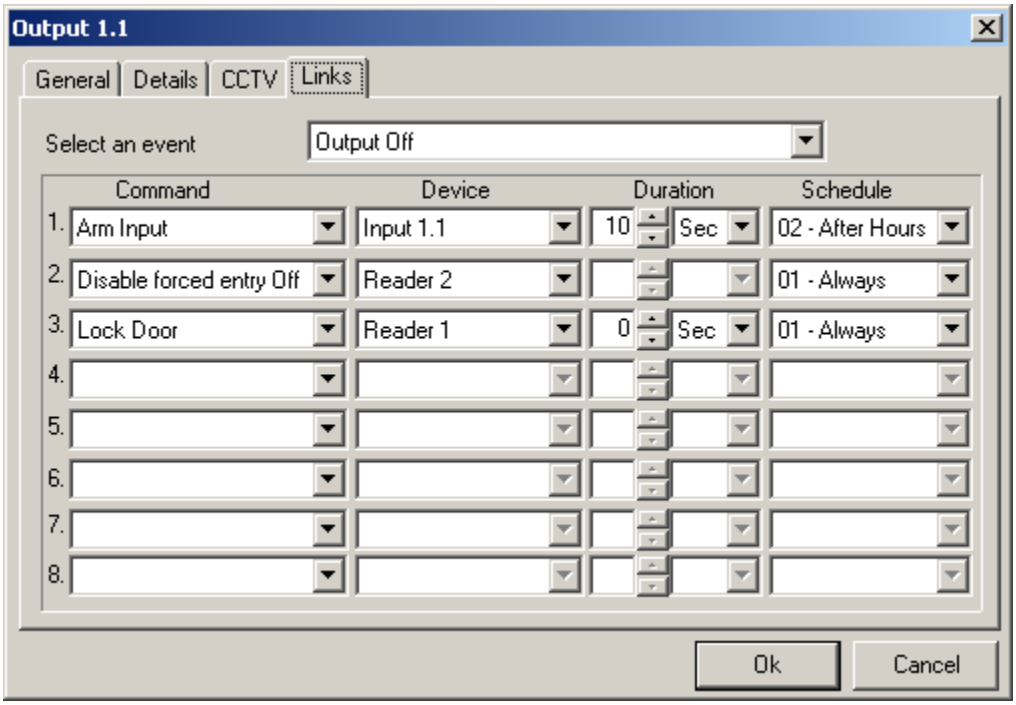
The second way the interface can be used is to associate with a specific DVR. DVR are set up in the *Database Screen* under DVR.

- First select a DVR for the pull down list under *DVR Name*.
- Next configure the *Camera Information*. Select a camera number, indicate whether it's a PTZ camera or not, and if it is enter a preset number if applicable.
- Then set the *History Information*. Set the *Pre Event Time*, and the *Post Event Time*. These times set playback start time (how much time before the event time) and the playback end time (how long to continue the playback after the event time).

This configuration is used by the History Reports DVR tab to playback video associated with a logged event.

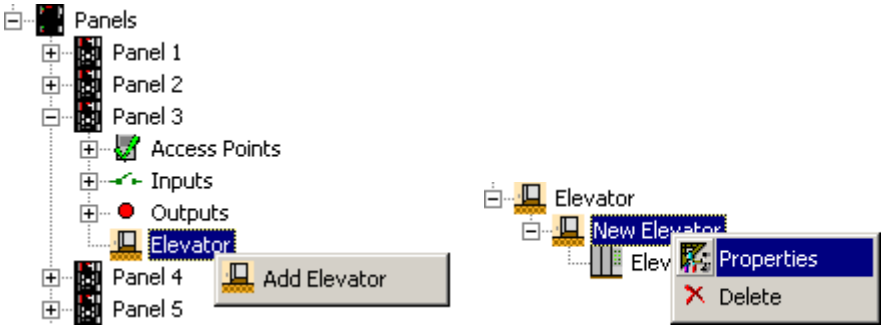
The *Links* tab is only available for programming for general-purpose outputs.

Links

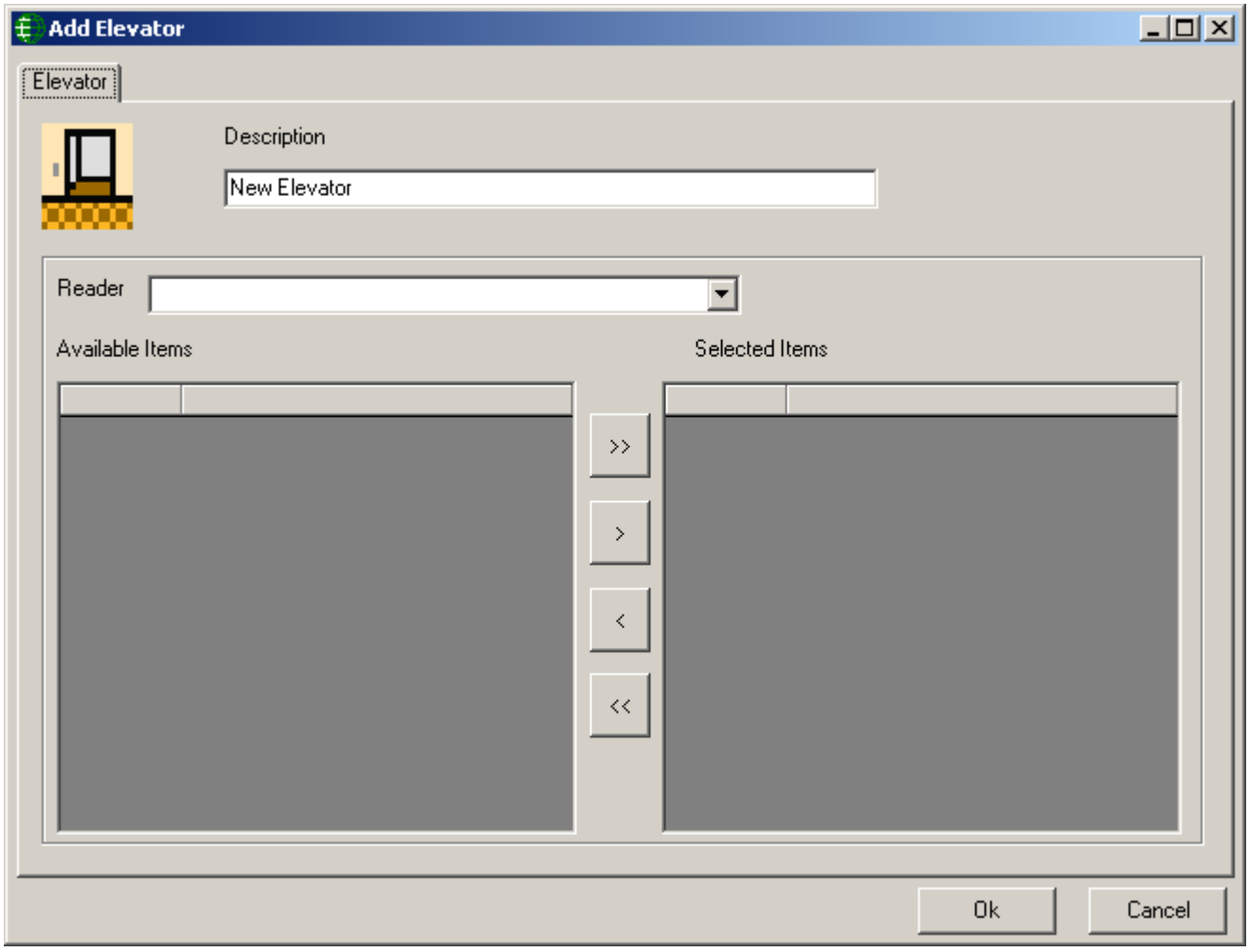


- First select an event.
  - Either Output On or Output Off.
- Then select up to eight commands to be executed with that event.
  - The command selection list includes; arming or disarming an input, turning on or off an output, locking or unlocking an access point, setting High Security mode on or off for an access point, and turning Disable Forced Entry on or off.
- After you have selected a command an appropriate device needs to be selected (*input, output, or access point*).
- Choose the duration of the command (*0-127 seconds or 0-126 minutes*).
  - Not all commands can be timed. *High Security* on and off, and *Disable Forced Entry* on and off cannot be timed.
  - A schedule can also be selected for each command (*the command will only be executed when the schedule is on*).

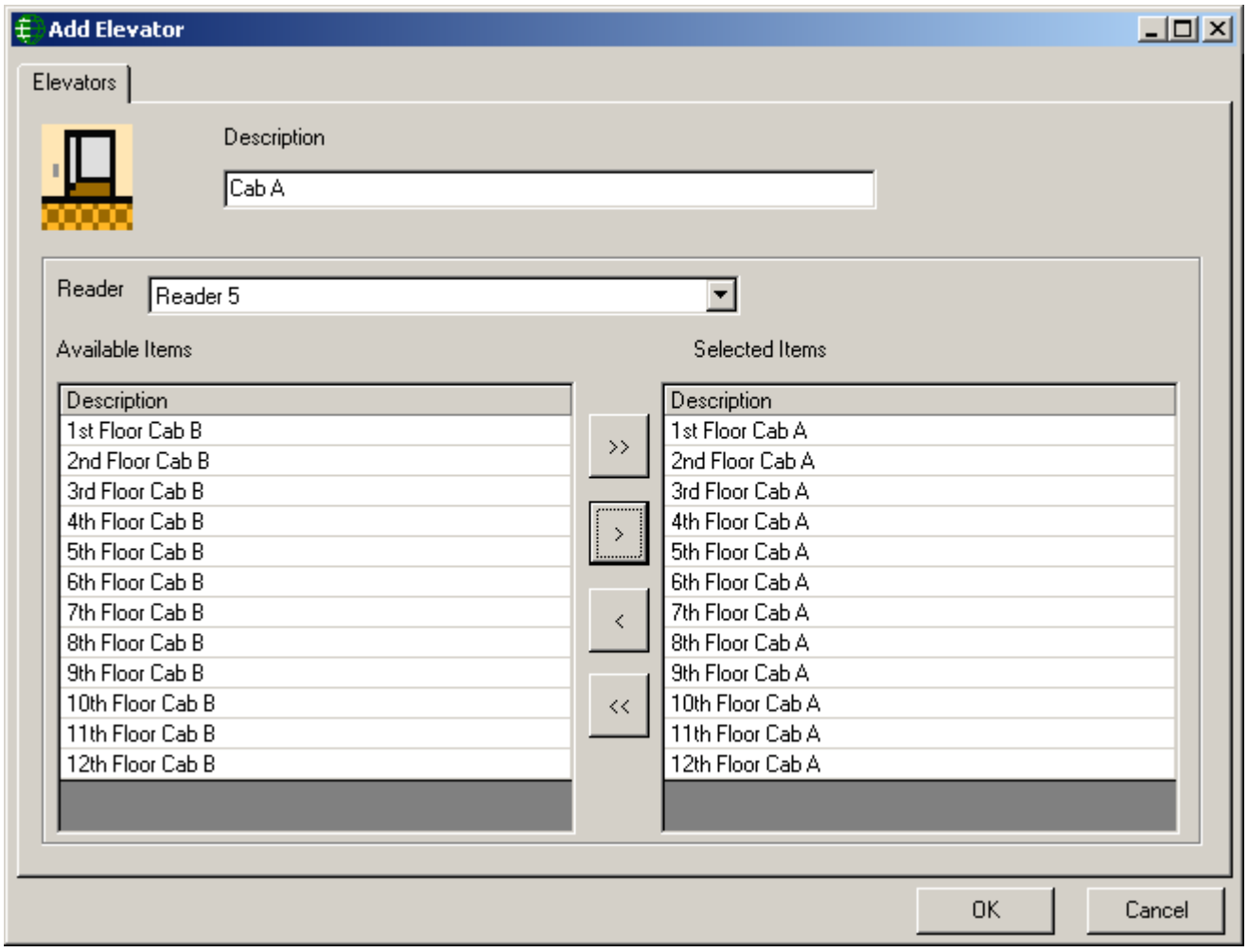
Elevators



The URC2000 Elevator Control can control up to two elevator cabs and thirty-two floors. You can split the thirty-two floors between the two doors any way you like.

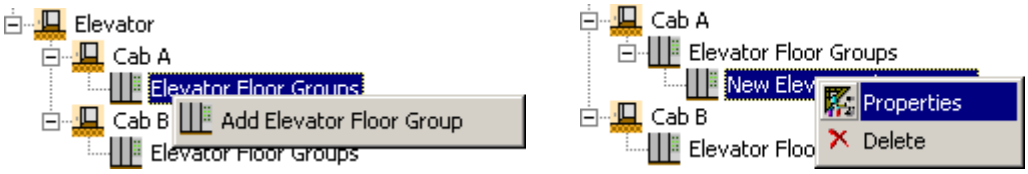


Access Points used for elevator control will have all the standard functionality of regular Access Points except for Antipassback and Interlock, and unlocking these Access Point will only affect the outputs assigned to the URC2000 controller and not the floor outputs.



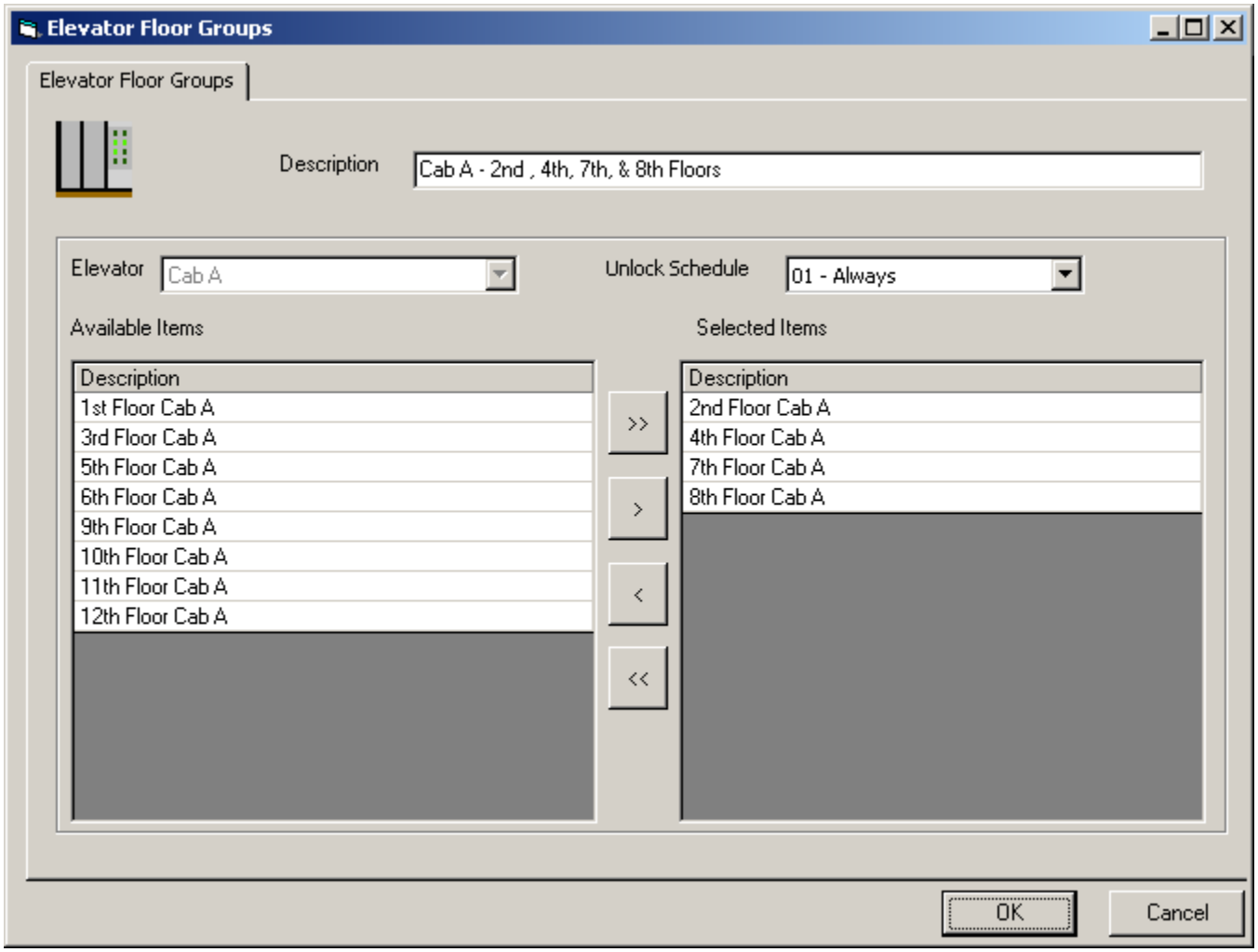
Change the Description, select a reader, and for that reader determine which outputs (*floors*) are to be controlled on this elevator. You can create up to two elevators (*per controller*) by using both the A side and B side readers.

Floor Groups



Add Floor Groups as required. Change the description and select which floors are to be member of the group. Each group can be given an Unlock Schedule so that its floors can have free access during that time.

Only fifteen Floor Groups can be created for each elevator.



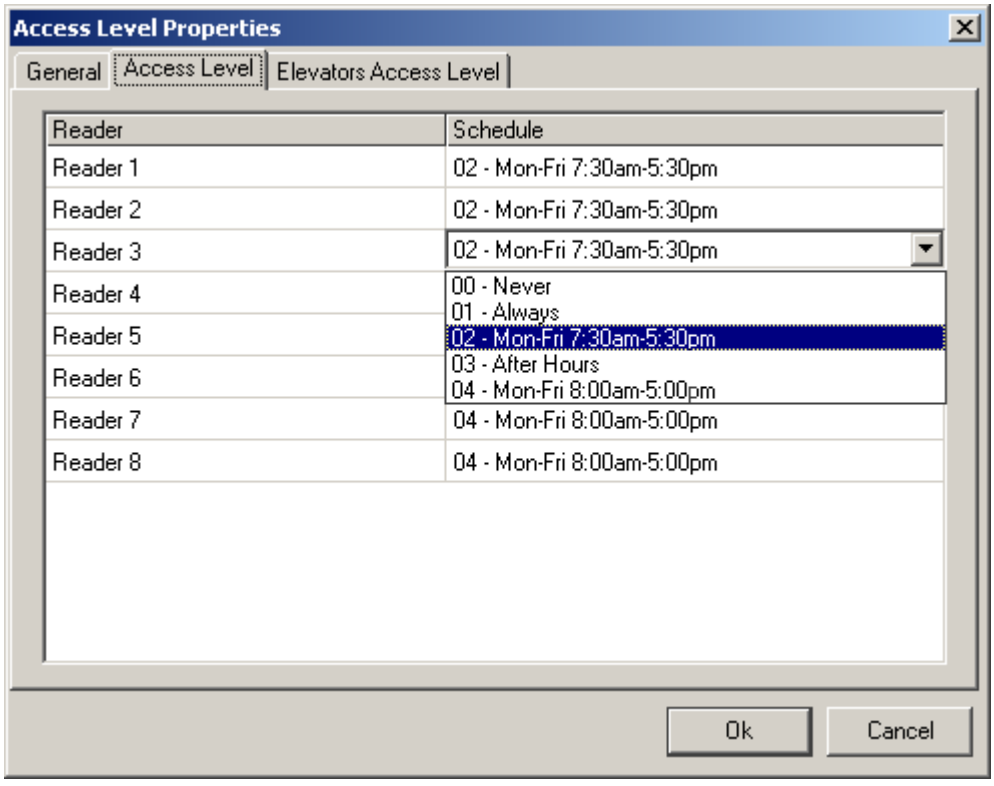
Access Levels

Assigning schedules to access points and floor groups creates access levels. They are created so that cardholders can be easily given access rights. Before cardholders are entered, any additional access levels that are required should be programmed. The only default access level is *Master*, which always provide access to all doors and all floors.

General

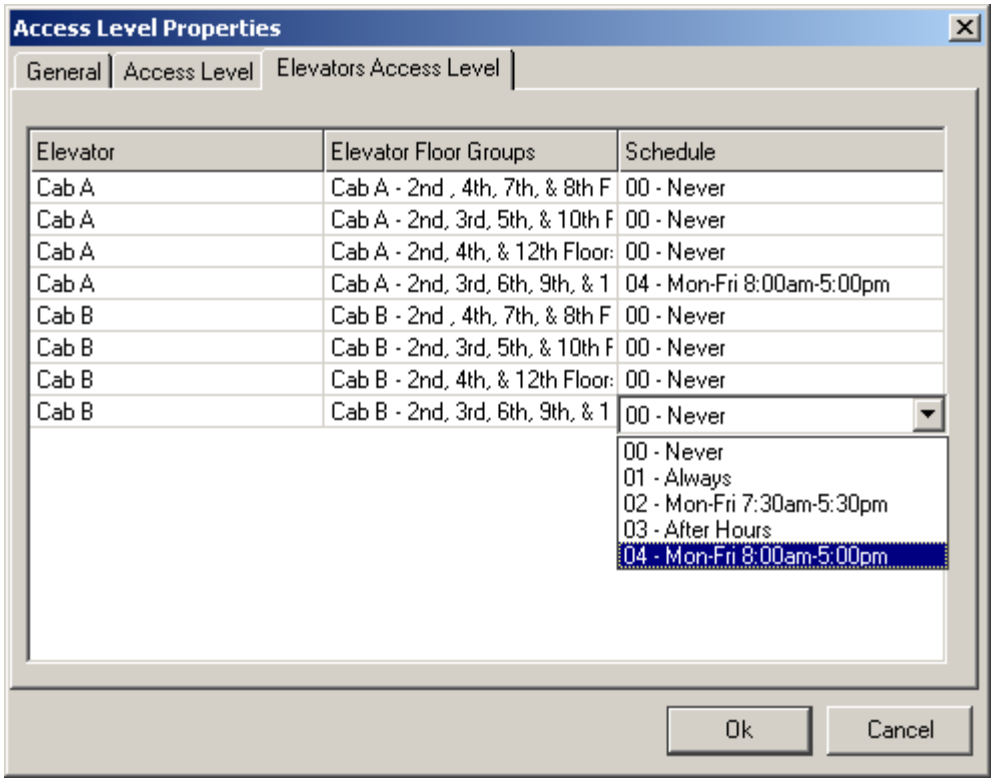
Change the *Description* of the *Access Level* in the *General* tab.

Access Level



Program the *Schedule* corresponding to the Reader (*e.g. front door & rear door*) in *Access Level* tab. Assign one schedule to each access point. Use the Never schedule if no access is be allowed at the access point. Any access points added after the creation of the Access Level will be given the schedule *Never*. Access levels can easily be edited anytime after they are created if changes are required.

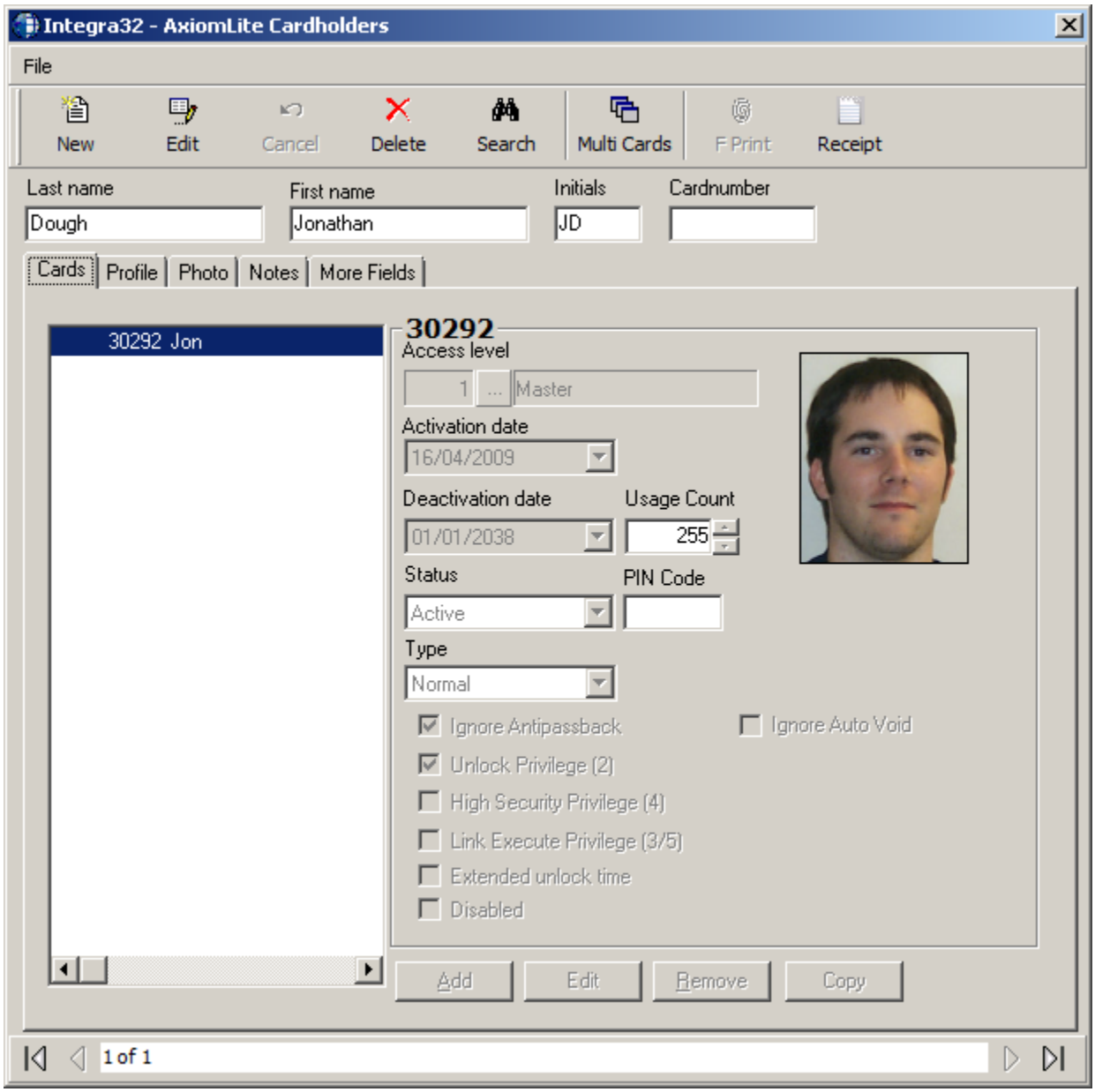
Elevator readers require a schedule but the actual schedule selected is irrelevant. The actual Cardholder's access is determined by the Schedules on the Floor Groups.



The schedule of any Floor Group can be changed to any schedule, as long as no more than **four** schedules are changed from Never. If multiple Floor Groups, that are given schedules, have floors in common than the cardholder will have access to those floors if any schedule allows it.

Chapter 6
Cardholders

Cardholders are entered/edited by clicking the *Cards* button from the toolbar of the *Main Window*.



Fields and Options

The cardholder window contains following fields and options:

File

Exit: Select this option to leave the Cardholder screen.

New

To add a new cardholder click on the *New* button, then the cardholder's information can be entered.

Edit

To make changes to an existing cardholder click *Edit*, then make the necessary changes.

Save

To save changes made to a cardholder click *Save.*

Cancel

Cancel will exit the edit mode without saving any changes to cardholder.

Delete

Cardholders that are no longer required can be removed from the database with the *Delete* button. All cards with this cardholder are deleted with it.

Search

To search for a cardholder click *Search*. There are many fields to search by, select one and enter your perimeters then click *Search.*

Multi Cards

Multi Cards will open a utility to add multiple cards in a sequence to the cardholder utility as well as to the panels.

F Print[21]

F Print will open the Touchstar finger print registry screen.

Last Name

Enter the cardholder's surname.

First Name

Enter the cardholder's given name.

Initials

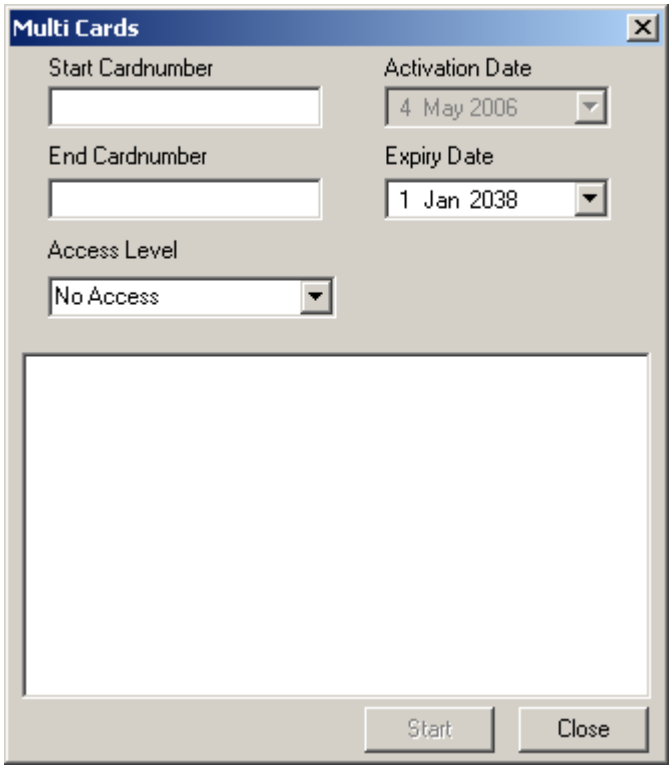
Up to six characters can be entered.

Cardnumber

Enter a number here to be used as a search parameter.

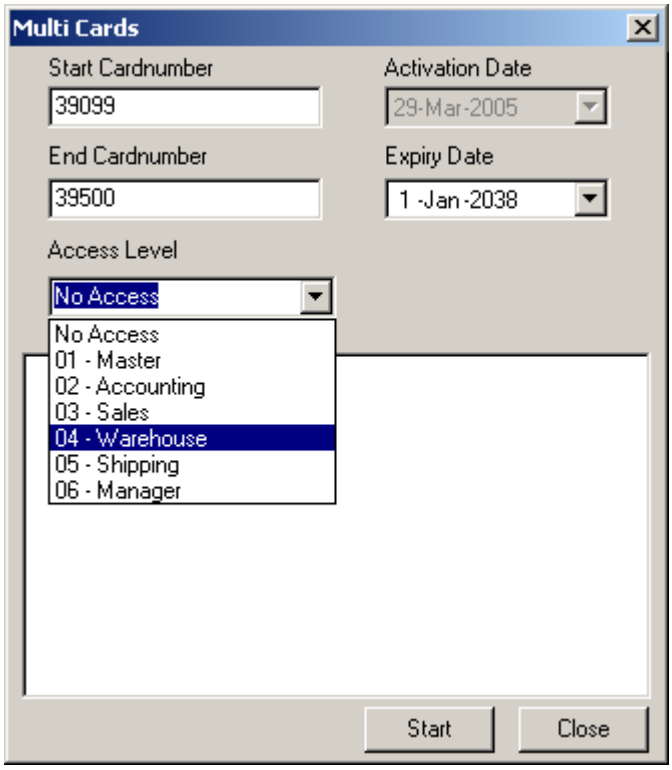
[21] This selection is only available if the optional license for the Finger Print Reader has been purchased and installed.

Multi Cards

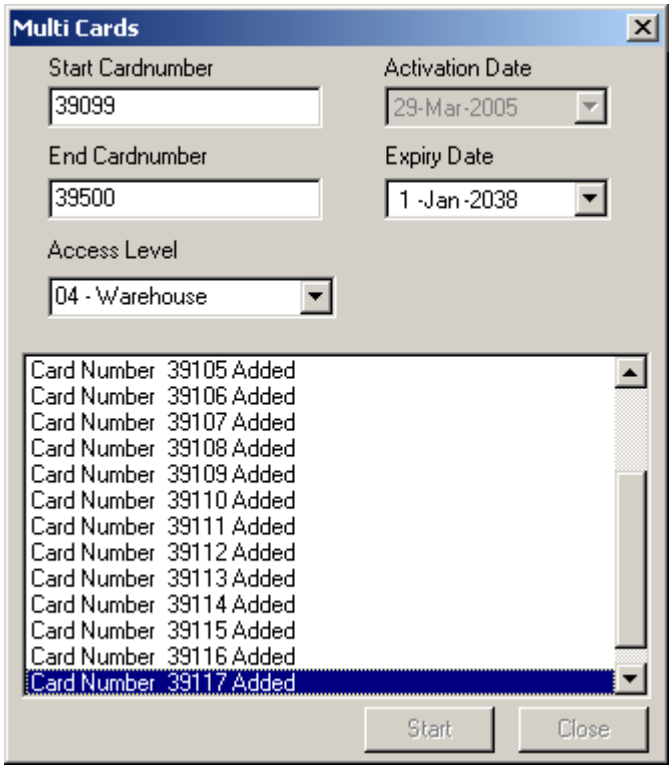


Multi Cards utility can add multiple cards in a sequence in the cardholder window as well as download them to the panel on the basis of the Access Level assigned to them.

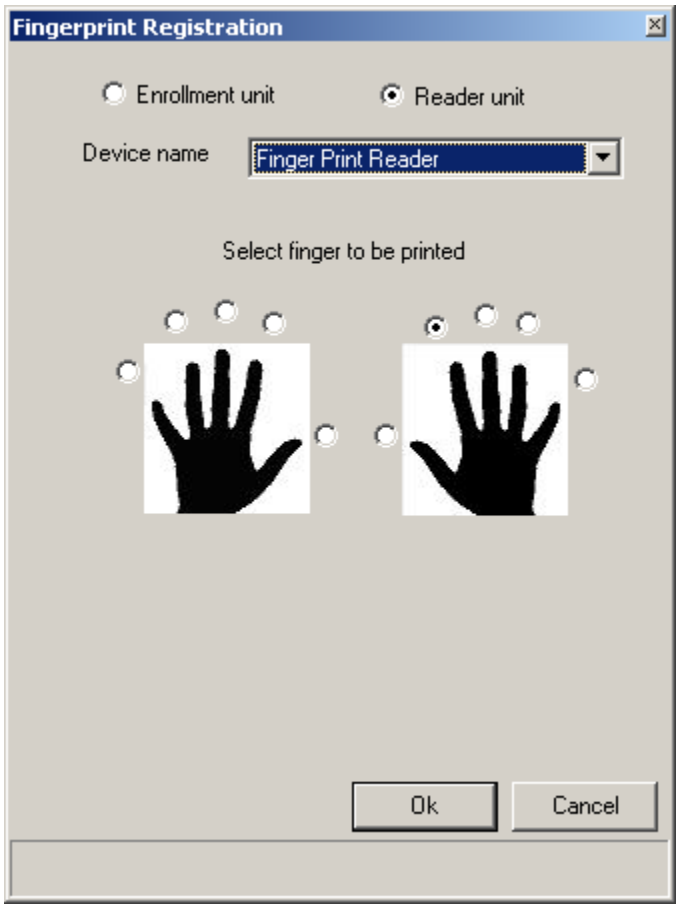
- Put in the Start and End card number.
- Assign the Expiry date, if any.
- Assign the Access Level from the drop down menu of the Access Levels configured in your system.



- Click on Start button to add the cards



F Print[22]

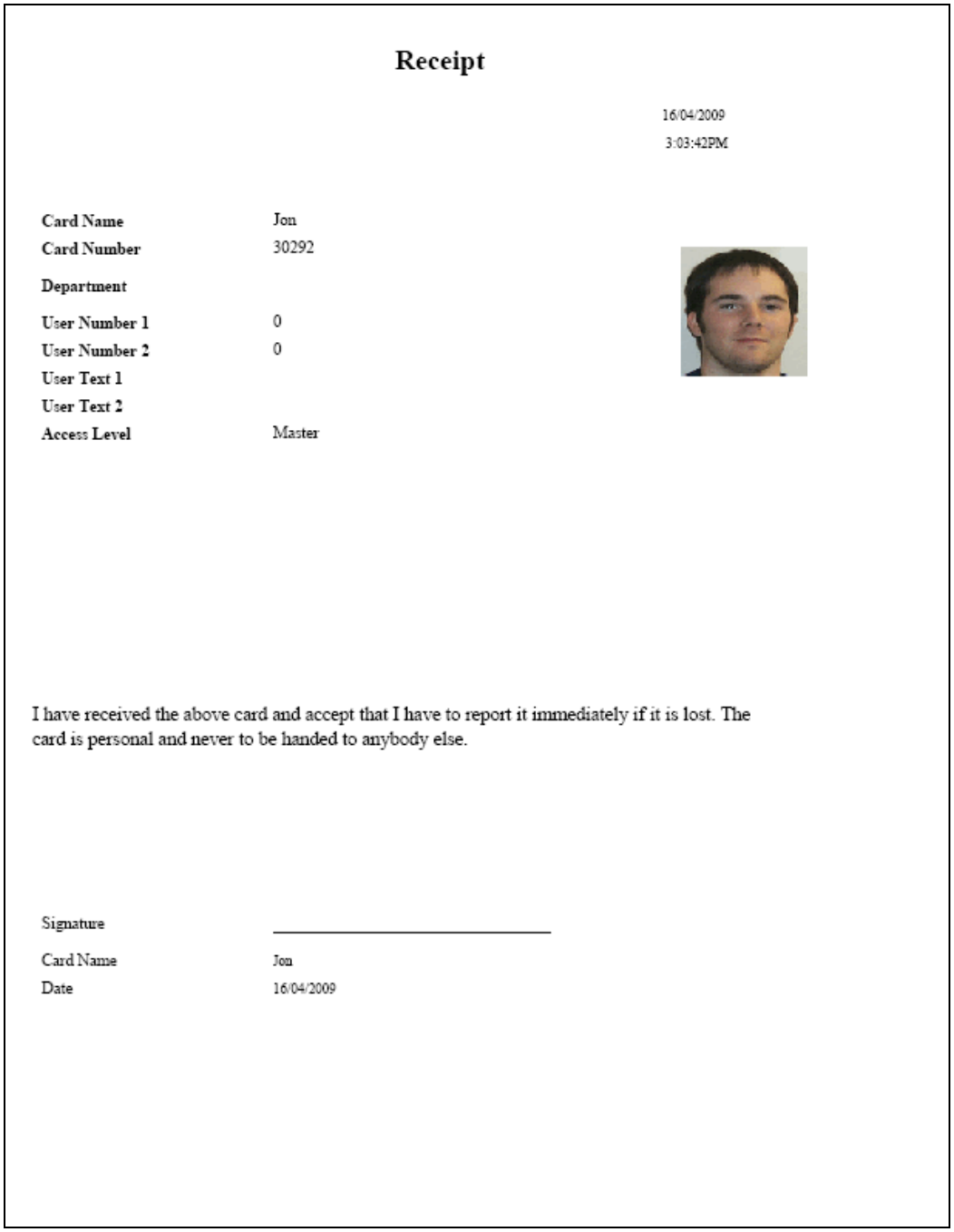


Use the RBHBIO-002 reader software to enroll/register finger print data.

[22] This selection is only available if the optional license for the Finger Print Reader has been purchased and installed.

Receipt

Receipt will create a printable document for the cardholder to sign indicating that the cardholder has taken possession of the card.



Receipt

16/04/2009
3:03:42PM

Card Name	Jon
Card Number	30292
Department	
User Number 1	0
User Number 2	0
User Text 1	
User Text 2	
Access Level	Master

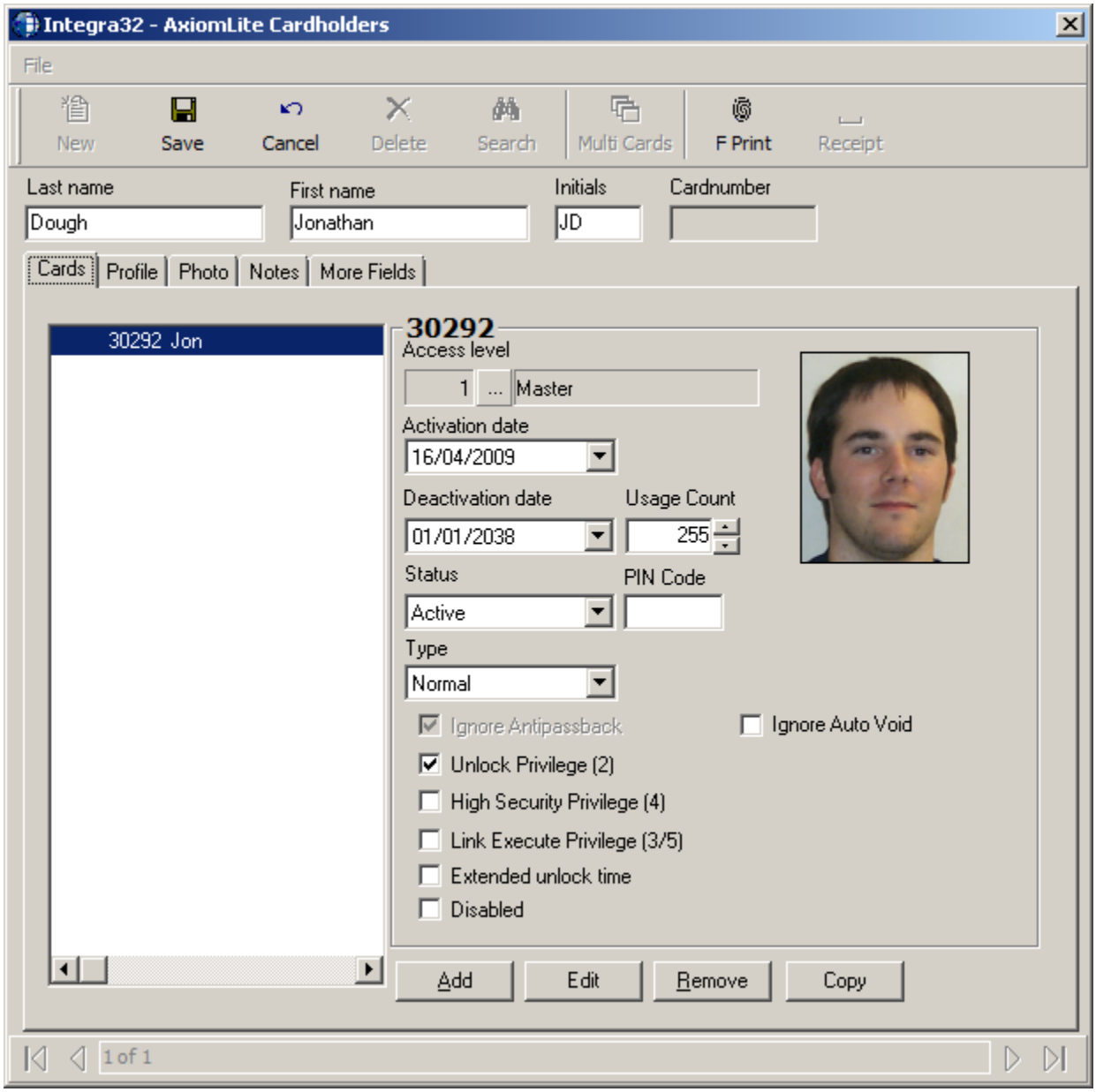
I have received the above card and accept that I have to report it immediately if it is lost. The card is personal and never to be handed to anybody else.

Signature	_____
Card Name	Jon
Date	16/04/2009

Cardholders' Tabs

Cards

Since cardholders can have multiple cards, card features will only be shown for selected (highlighted) card number only. When adding or editing cards ensure that the proper card number is selected (highlighted).



Access Level

Select previously defined access levels from the pop-up window. Access levels determine when and where an access code is valid.

Activation Date

MM-DD-YYYY[23]. This field is automatically populated with the current date and time when a new cardholder is added to the system.

Deactivation Date

MM-DD-YYYY[24]**.** To deactivate a cardholder, enter the current date, or a date in the future, on which that cardholder is to be deactivated. The cardholder will be deactivated automatically on the specified date. This field defaults to 1 January 2038.

Status

Card status is shown here, generally active or inactive (*depending on the activation and deactivation dates*). This status can be changed to stolen, destroyed, expired, lost, or suspended.

Usage Count

Valid range is 1-255. Enter the maximum number of times the card can be used. It reduces the count by one, every time the card is used (*at specific readers*) to gain access. When the count reaches zero the card can no longer be used. To specify that a card is valid for unlimited number of uses, enter 255.

Pin Code

The PIN - Personal Identification Number - is the code required at access points with a keypad.

Type[25]

There are currently only two card types to choose from, normal, and visitor. Normal cards are for your regular permanent cardholders while visitor cards are for a group of continually changing cardholders. These cardholders are people who only need a card for a short period of time; they use the card while they are on site and then hand it back in when they leave.

Options

Choose from the six options available, if required: *Unlock Privilege, High Security Privilege, Link Execute Privilege, Extended Unlock Time,* and *Handicap, Ignore Auto Void.*

Ignore Antipassback

Cards that are given this option will bypass antipassback checks when presented to a reader. (This option can not be independently selected but is given to a cardholder that has been given Unlock or High Security Privilege.)

---

[23] Date is displayed in the format selected under Windows – Control Panel – Regional Settings Properties-Date. If a two-digit year was chosen then it will be displayed in that form here.

[24] Date is displayed in the format selected under Windows – Control Panel – Regional Settings Properties-Date. If a two-digit year was chosen then it will be displayed in that form here.

[25] This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

Unlock Privilege (2)

Cards with this option can unlock or lock access points with a double grant access. Two consecutive grant accesses by the same card can toggle the lock/unlock mode of an access point.

High Security Privilege (4)

Cards with this option will be granted access on doors in high security mode. As well high security mode on a door can be toggled with four consecutive grant accesses.

Link Execute Privilege (3/5)

Cards with this option can execute *Global Links* with either three or five consecutive *Access Granteds*. Three consecutive *Access Granteds* can be programmed with a different link then five consecutive *Access Granteds*.

Extended Unlock Time

Cards with this option will use the *Extended Unlock Time* instead of the regular *Unlock Time*.

Disabled

Cards with this option will activate the *Handicap Output* associated with the access point. The *Handicap Output* follows the activation of the *Lock Output* by a short delay, and is used to trigger a door operator to open the door.

Ignore Auto Void

Cards with this option will ignore Auto void, if selected any in system settings.

Cards

Up to twenty cards can be added per cardholder. New cards can be added for an existing cardholder with the *Add* button. All the cards assigned to a cardholder can be seen on the left-hand window of the *Cardholder Screen* when a cardholder is selected. The card number and description of the card are put into this window.

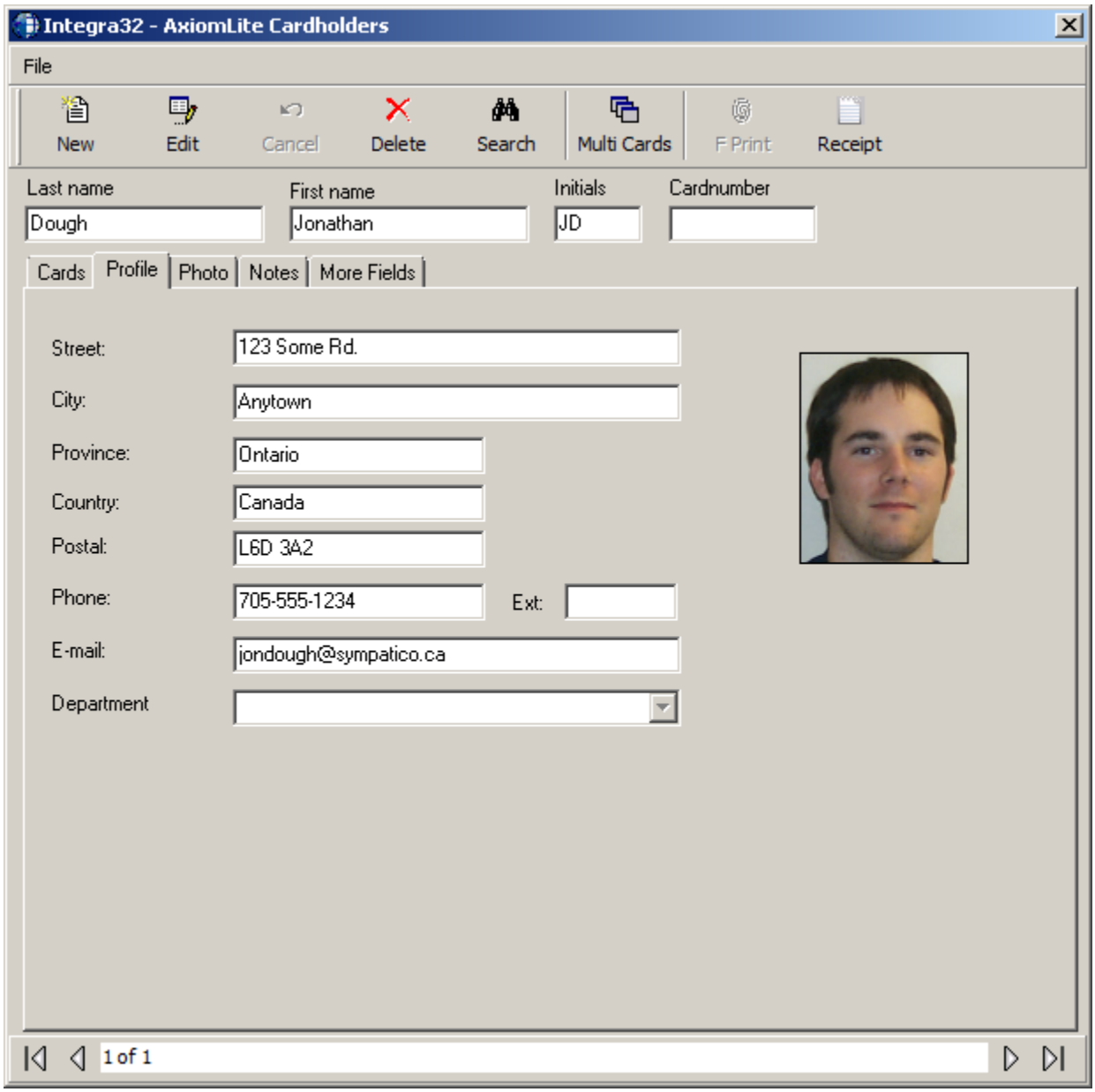
Click the *Add* button to add a card to the cardholder. Enter the card number in *Value*. *Name* is optional and is used to distinguish a cardholder's different cards from one another. Click OK to enter the card number.

Copy will enter a new card, with a different *Value*, and an activation date of the current date. All other parameters will be the same as the selected (*highlighted*) card.

Use the *Edit* button to edit the description of any card assigned to the cardholder, and use the *Remove* button to delete a card assigned to the cardholder.

Profile Tab

The profile information (*like address, phone number and email address*) of a cardholder can be entered in the *Profile* tab. All of this data is optional, and does not affect the functioning of the Access Control System.



Department can be selected form the pull down list instead of being typed in.

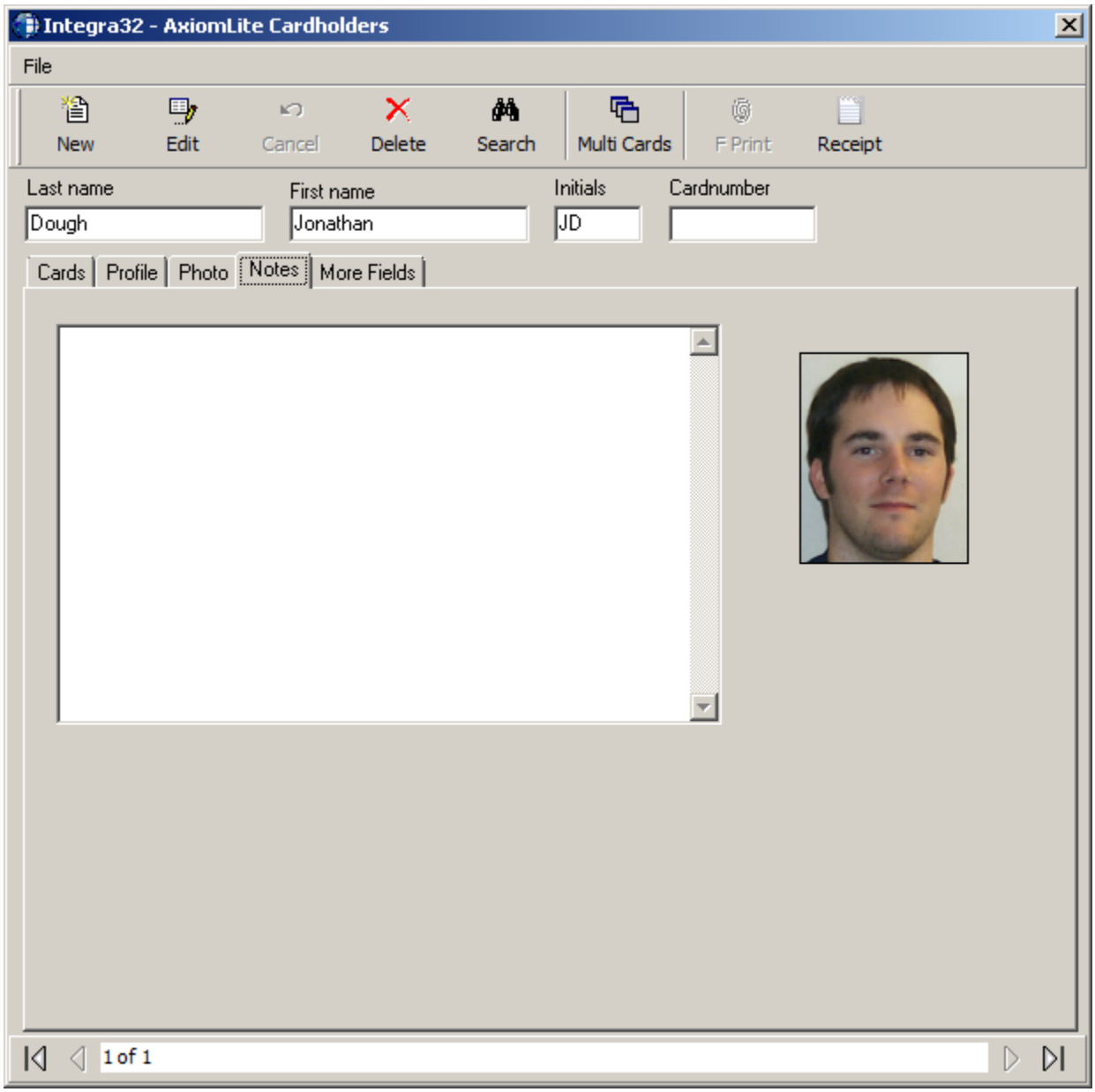
Photo Tab

You can select an already saved picture of the cardholder in the Photo tab or you can acquire a cardholder's image. The picture is then saved in the Integra32\Images folder. You can select or print one of the already saved templates for the cardholder in this tab if the badging option is part of the software.

Use the Card Front and Card Back buttons to view both sides of the badge.

Notes Tab

Any other relevant information concerning a cardholder can be saved under the *Notes* tab.



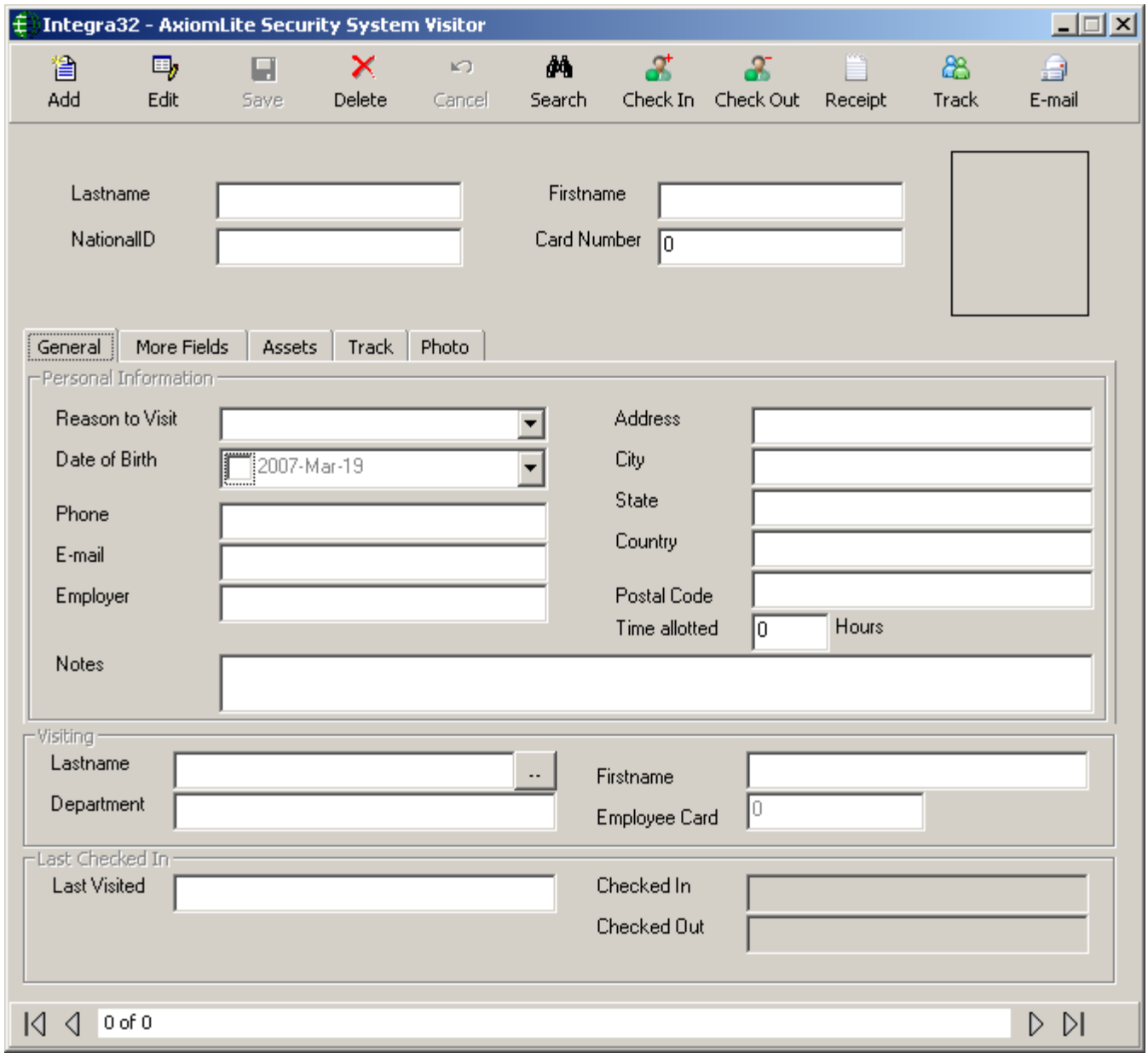
Notes entered here can be displayed in Access Point Activity window when it is expanded to show *More*.

More Fields Tab

Any additional information required for cardholders can be saved in *More Fields* tab. The user can rename the fields under this tab by right clicking on the label to be renamed. There are two numeric fields, six text fields, and two date fields for the user. These fields can be used in searches and can be displayed on badges.

Chapter 7
Visitor Manager [26]

To add a visitor into the system the card they are to use must first be entered into the cardholder screen and configured to *Type* visitor. The *Profile*, *Photo*, and *More Fields* tabs are actually redundant to visitor cards. The *Cards* tab of course is required while the *Notes* tab is optional.



[26] This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

The Last Name and First Name fields are mandatory fields and must have data before you can save the visitor while the NationalID field is optional. All three of these fields are 'quick search' fields. Type data into the 'quick search' field and hit *Enter*. The 'quick search' field will call up the record with matching data or will produce a list of record to choose from.

Card Number is also a 'quick search' field and is ideal for calling up a record when a visitor is checking out.

Add

Click *Add* to enter a new visitor.

Edit

Click Edit to modify an existing visitor.

Save

Click *Save* to save changes made be adding a new visitor or modifying an existing one.

Delete

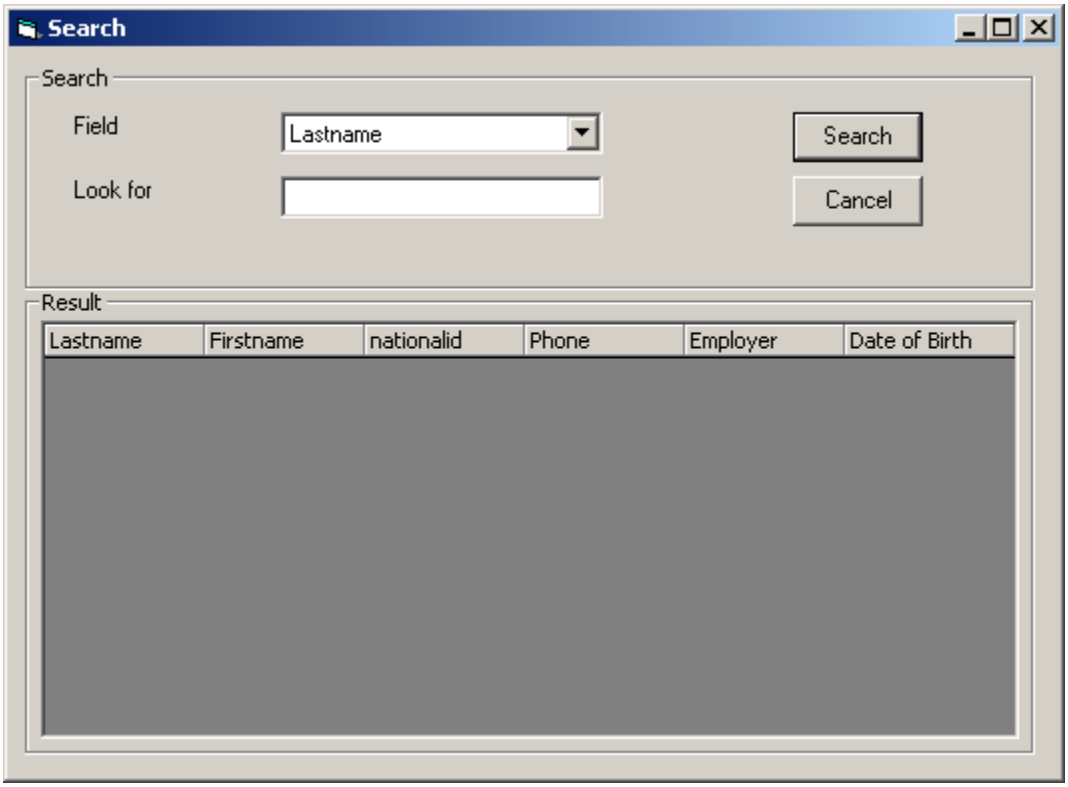
Click *Delete* to permanently remove a visitor from the database.

Cancel

Click *Cancel* to exit edit mode and not save any changes made.

Search

Click *Search* to call up a search screen to look for a specific visitor.



Select the search field, enter the search criteria, and click search. The results of the search will be posted in the lower half of the screen.

Check In

Click *Check In* to have the visitor check in to the system.

Check Out

Click *Check Out* to have the visitor check out of the system.

Track

Click *Track* to display the access points that the visitor has been granted access to while checked-in.

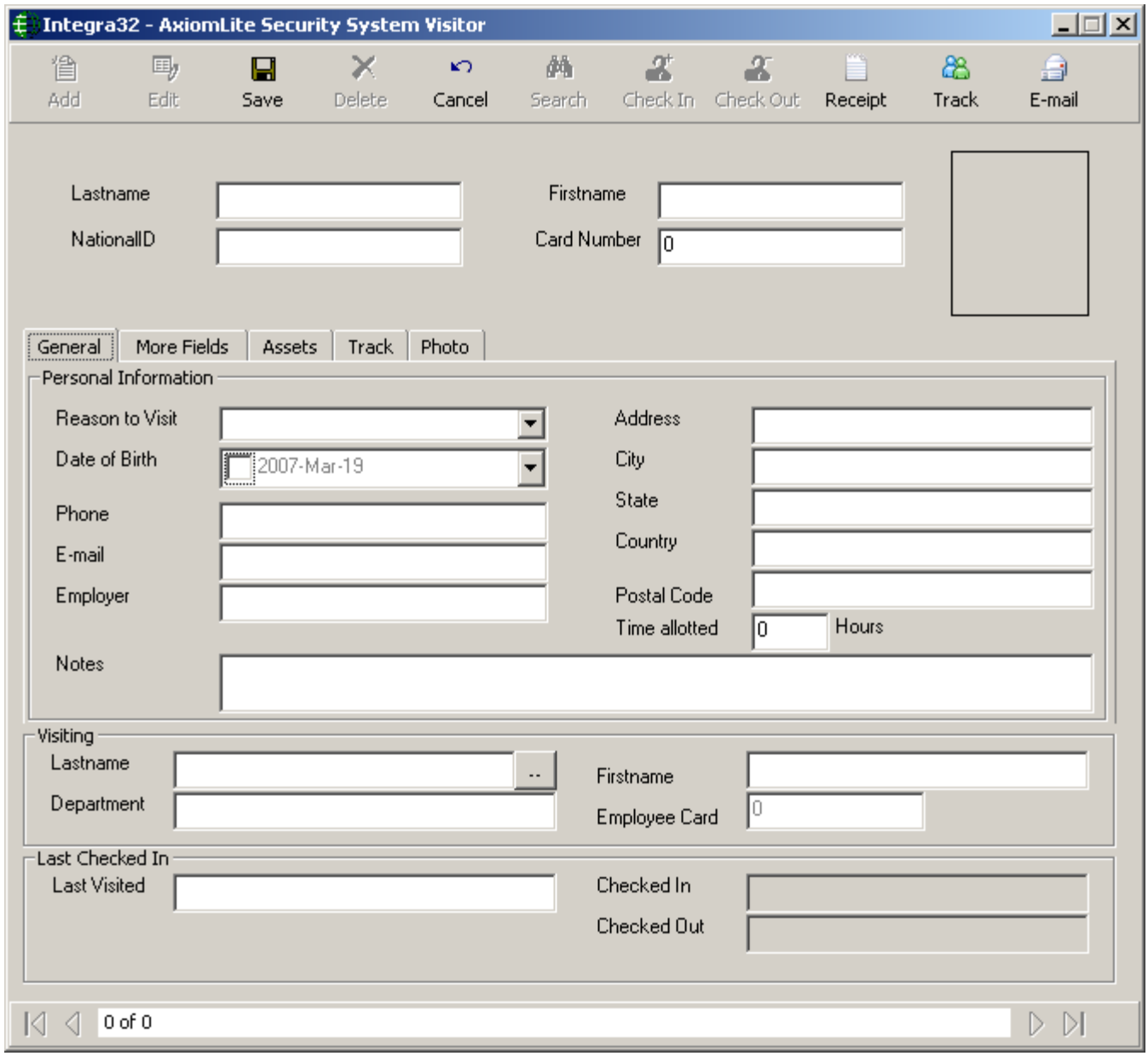
Receipt

Click *Receipt* to print a receipt for a visitor's assets.

E Mail

Click on *E Mail* to send an email to the cardholder being visited. For this to work the senders email information must be configured in VM Configuration under eMail Configuration and the being visited cardholder's Profile Tab must have an email address.

General

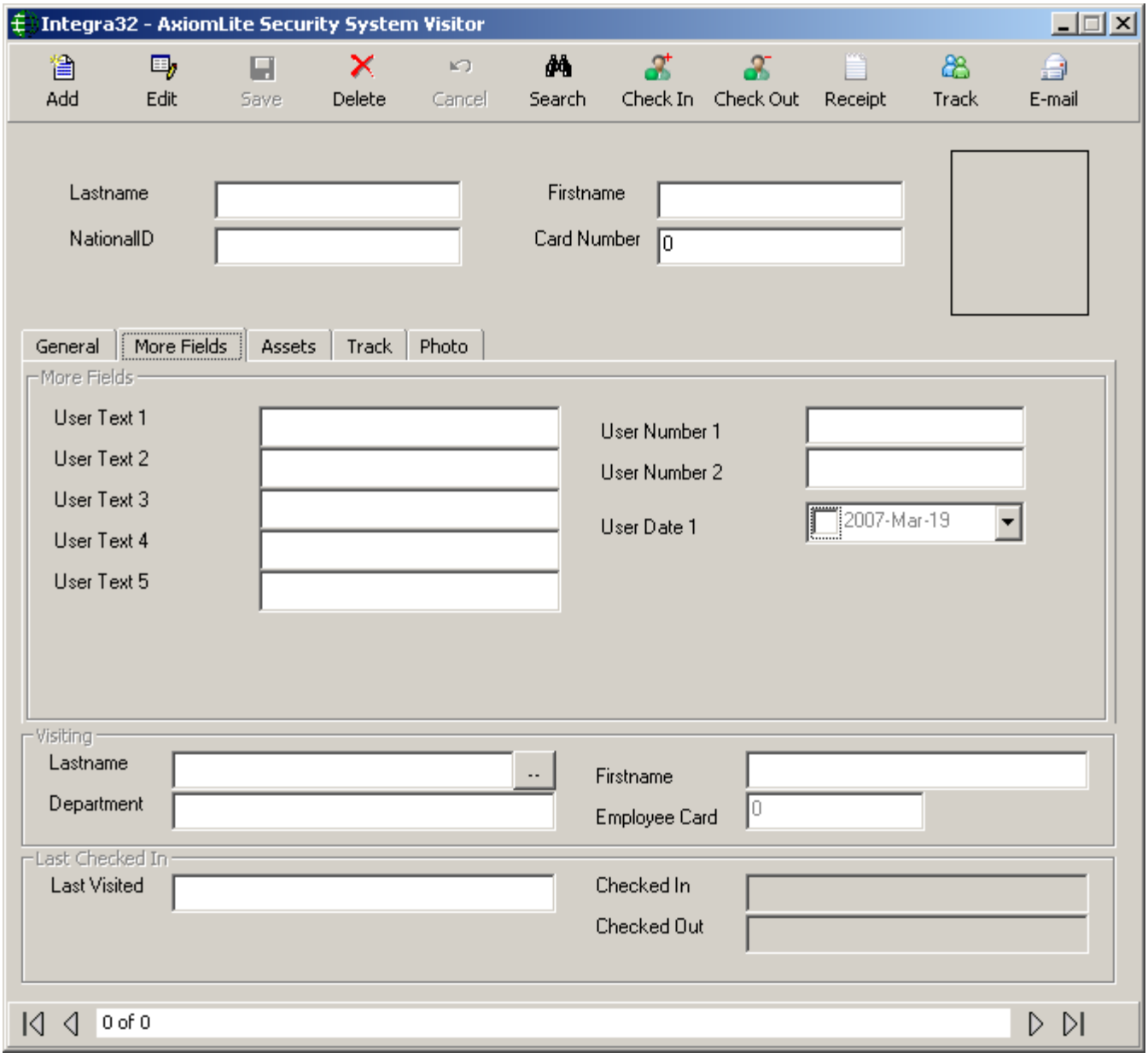


Personal Information data is optional and specific to the visitor and not to the card.

Select who is being visited by clicking on the browse button [**..**] and search for the appropriate cardholder. *Department* and *Employee Card* will be filled in by the system.

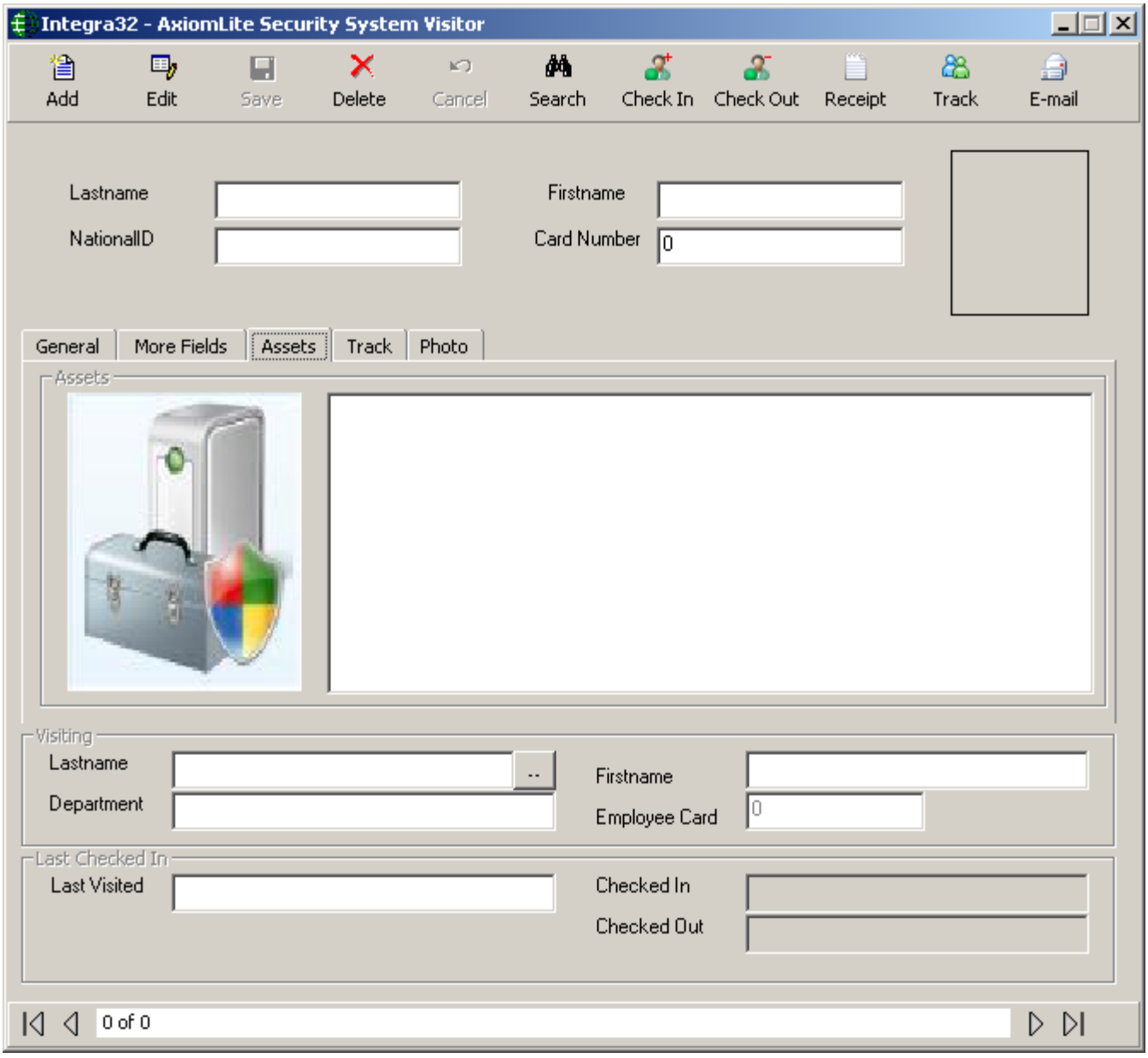
Last Check In is also filled in by the system.

User Fields



User Fields are customized fields to hold data pertaining to your visitors. The headings for these fields are set in VM Configuration under the User Fields tab.

Assets

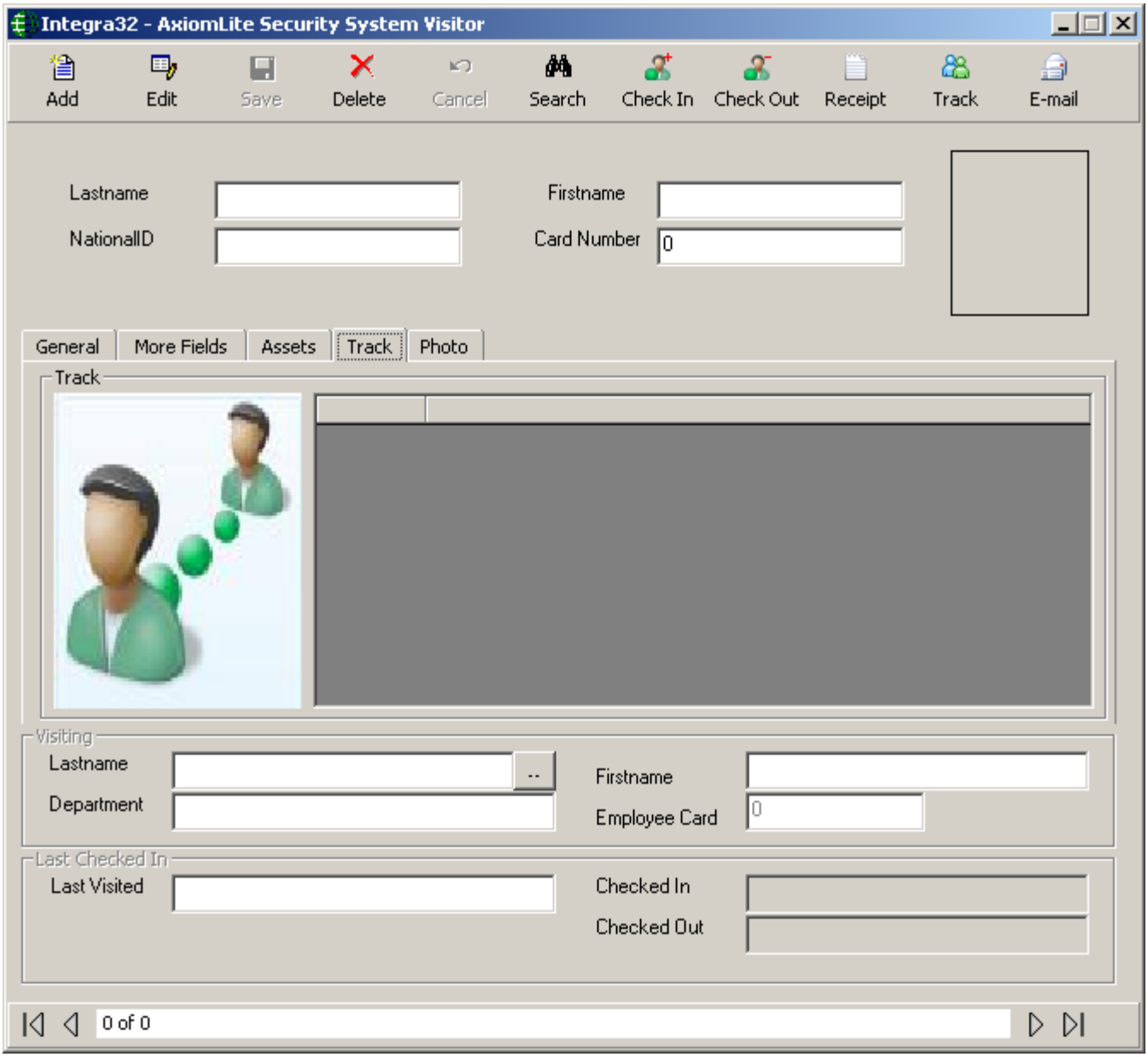


Under the *Assets* tab, in edit mode, the operator can enter data concerning anything that the visitor brought with them to the site.

To print a receipt for these assets click on the *Receipt* button.

If there is any information entered under a visitor's asset then a reminder will pop up when the visitor checks out. After the visitor has checked out this asset data is deleted.

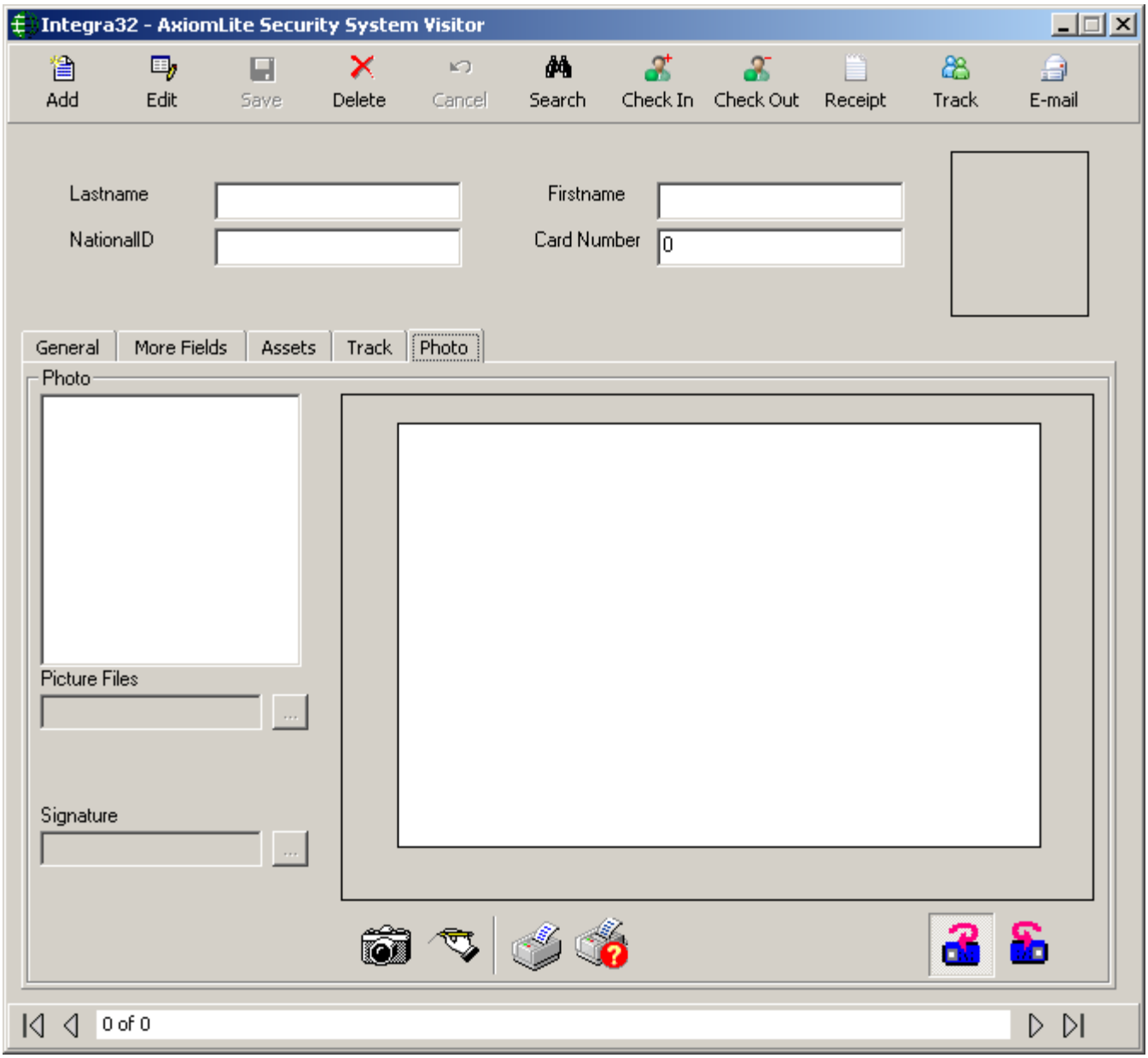
Track



The *Track* tab will display the access points that the visitor has been granted access to since their check-in time. Simply click on the track button to display the information.

Only visitor that are checked-in can be tracked. If the visitor has checked-out you can get information on where they have been from the Visitor Reports.

Photo



The *Photo* tab shows all the templates from the badging template module. Only the fields valid for the visitor management will be shown on the badging templates in this module.

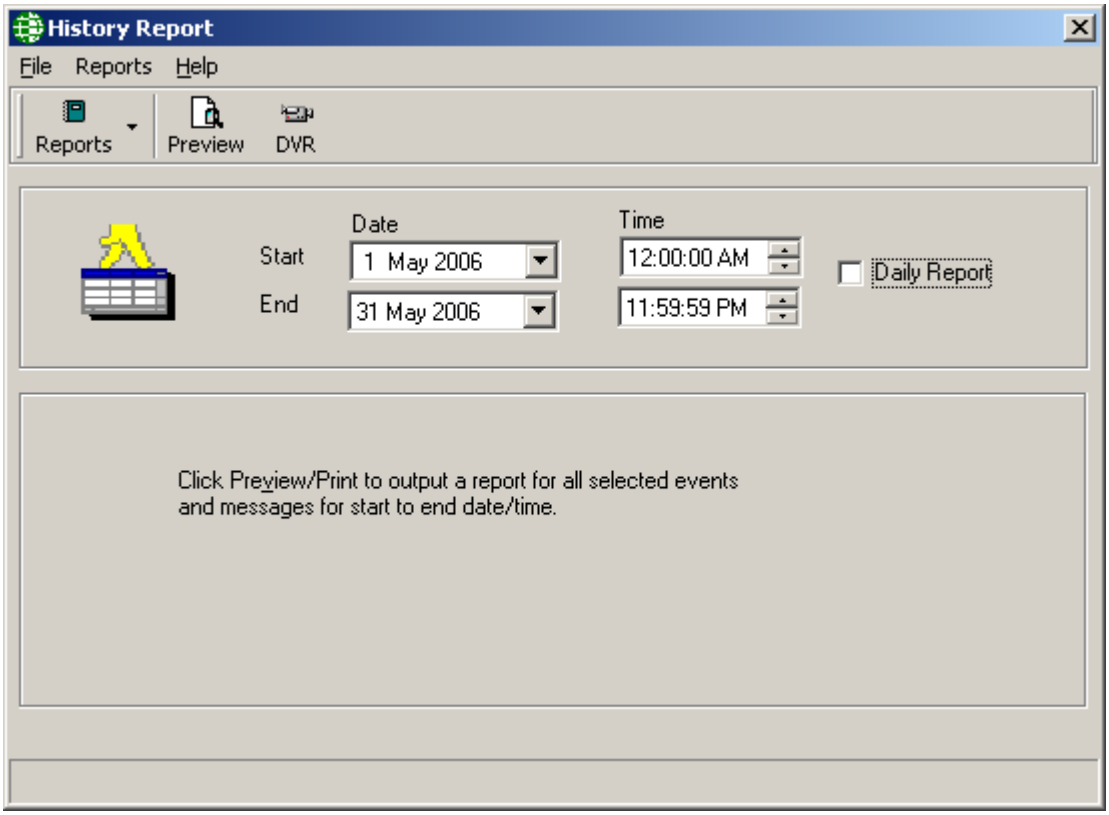
Chapter 8
Reports

The Integra32™ report creation facilities allow you to customize an almost unlimited number of reports and can be used as an extremely valuable management tool.

From *Reports* menu you can choose to launch *History Report* or *Database Report Window*.

History Reports

Select *History Reports* from the *Reports* menu to launch the following window, where the user has the option of selecting from many history reports available.



File

From the file menu the user can *Print, Select History Path* or *Exit* from the History Report window.

Print

The *Print* command will produce a printed report showing the data selected for the chosen report.

Select History Path

If your history files are not being saved to the Integra32 folder, then the path to their location will be required.

Reports

The user can select the kind of report they want to preview or print from the *Reports* menu. The options available are: *Main, Card Holders, Access Points, Inputs, Outputs, Controllers, Alarms, Operators, Time & Attendance, and Card Holder Simple*.

The same options are available from the *Reports* button of the toolbar.

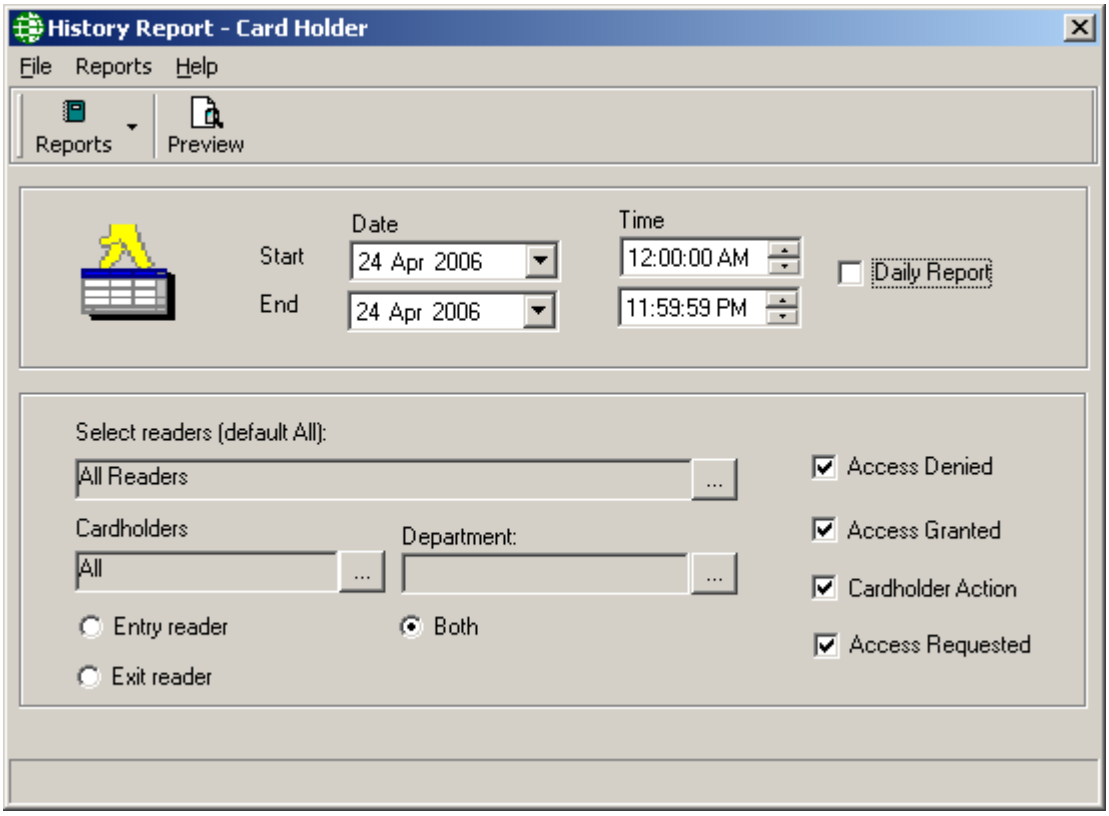
The user sets the *Start Date, End Date, Start Time,* and *End Time* for any report they have selected to preview or print. The report will span from the start time of the start date to the end time of the end date unless the daily report box is checked. If the daily report box is checked then the report will still span from the start date to the end date, but only include the times between the start time and end time of each day.

Preview

Clicking the *Preview* button of the toolbar, the user can preview or print any of the selected reports for selected time period.

To understand the *History Reports Window* in detail, let's take the example of one of the selected options: *Cardholders*

From *Reports* menu or *Reports* button, select *Cardholders* to show the following screen:



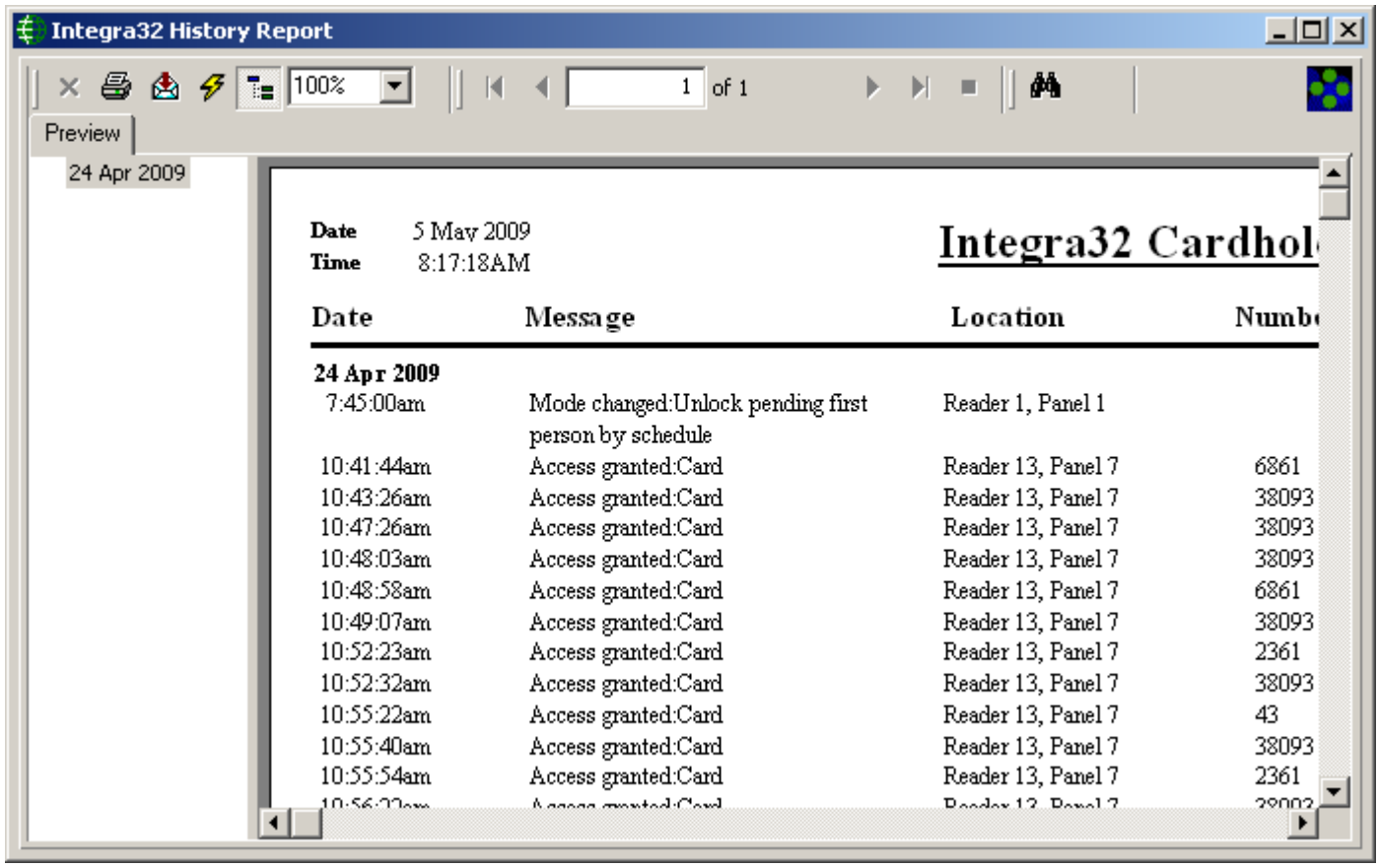
- Select the *Start* and *End*, *Date* and *Time* for the time period you want to preview the report for.
  - If the report is to cover only specific hours each day then check Daily Report so that the *Start* and *End Time* will be applied each day.
- Click the *Select Readers* button to select the readers you want on this report to preview or print. All readers will be shown by default.
- Click the *Cardholders* button to select cardholders for your report. All cardholders are selected by default.
- The user can customize the report by clicking in the checkboxes for *Access Denied*, *Access Granted*, *Cardholder Action*, and *Access Requested*. These selections will determine which messages are to be reported on.
- Click the *Preview* button to preview the customized cardholder's report.

Radio buttons: Select one of *Entry Reader*, *Exit Reader*, or *Both*. Readers are exit readers if they are connected to the Out Reader side of an Exit Reader Module or if their TAM terminal is grounded (IRC2000-4/-5 boards). Otherwise they are entry readers (this includes all readers on IRC2000-3/-2 boards)

⊙ Entry reader

⊙ Exit reader

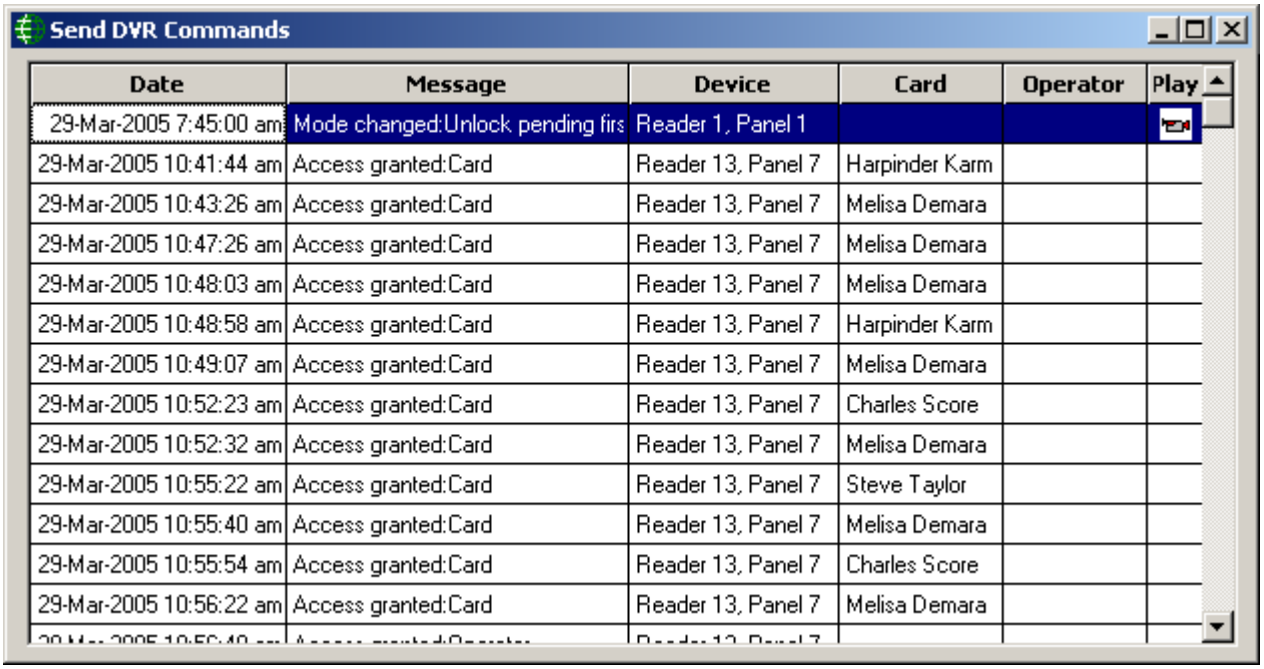
⊙ Both



From this report, the user has the option of *Printing*, *Exporting* the file, *Refreshing* the preview of the report, or changing the current view of the report.

DVR[27]

Clicking the *DVR* button from the toolbar of the *History Report* window, the user can preview *the Send Camera Commands* window to select the History Event Command he/she wants to send to the DVR.

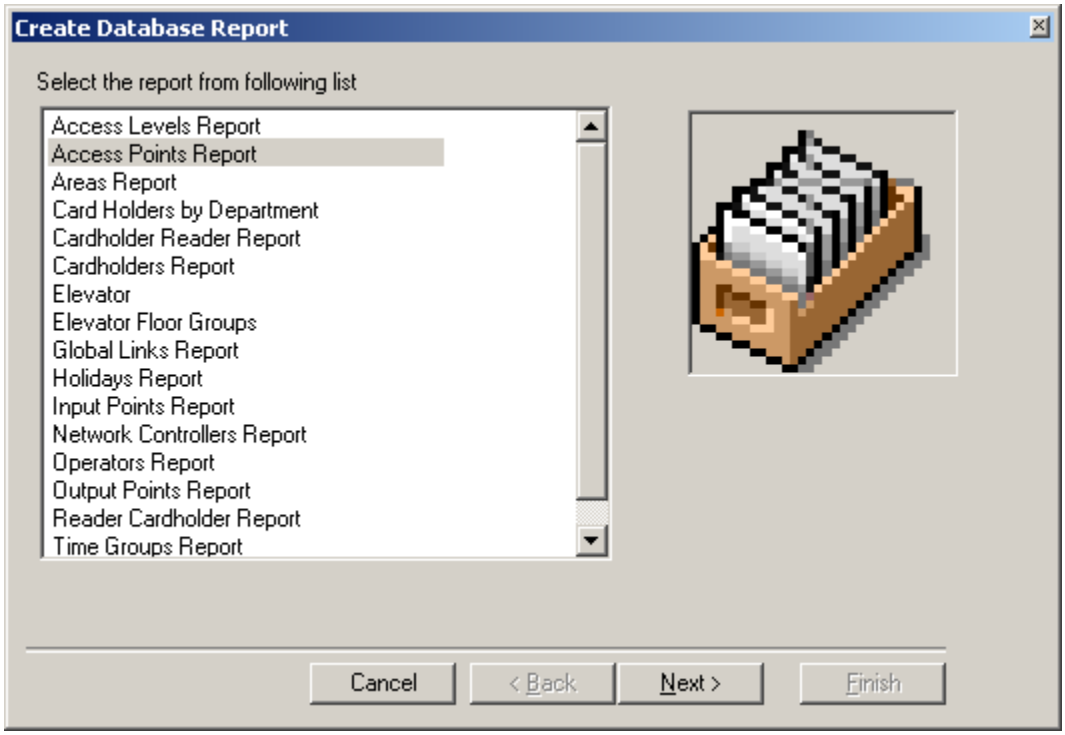


Double click the line that has a *Camera sign* , with the event that is to be played back.

[27] This selection is only available if the optional license for the DVR Software has been purchased and installed.

Database Reports

Select *Database Reports* from the *Reports* menu to launch the following window, where the user has the option of selecting from many database reports available.



Options

The options available for *Database Report* are:

- **Access Levels Report**
- **Access Points Report**
- **Areas Report**
- **Card Holders by Department**
- **Cardholder Reader Report**
- **Cardholders Report**
- **Elevator**
- **Elevator Floor Group**
- **Global Links Report**
- **Holidays Report**
- **Input Points Report**
- **Network Controllers Report**
- **Operators Report**
- **Output Points Report**
- **Reader Cardholder Report**
- **Time groups Report**

- Select one of the reports available (*e.g. Access Points Report*). Click the *Next* button to select the options available in for the chosen report:

- Select the items to include in the report or click in the check box for *Select All* if you want to include all the items available in your report.

- Click the *Next* button to select from the available fields to include in the report, or check the *Select All* box to include all fields.

    - By default four fields are selected. If up to five fields are selected a simple report will be produced. For more than five fields a detailed report is produced.

    - For some reports there is a main report and sub report. If you select *Show Subreport*, which is selected by default, the *ID* field cannot be unselected. It is required to link the main and sub report. The fields selected in this list are for the main report only. Up to ten fields can be selected. If you select more than ten fields the first ten will be shown.

- Click the *Next* button to select the sort order for the report

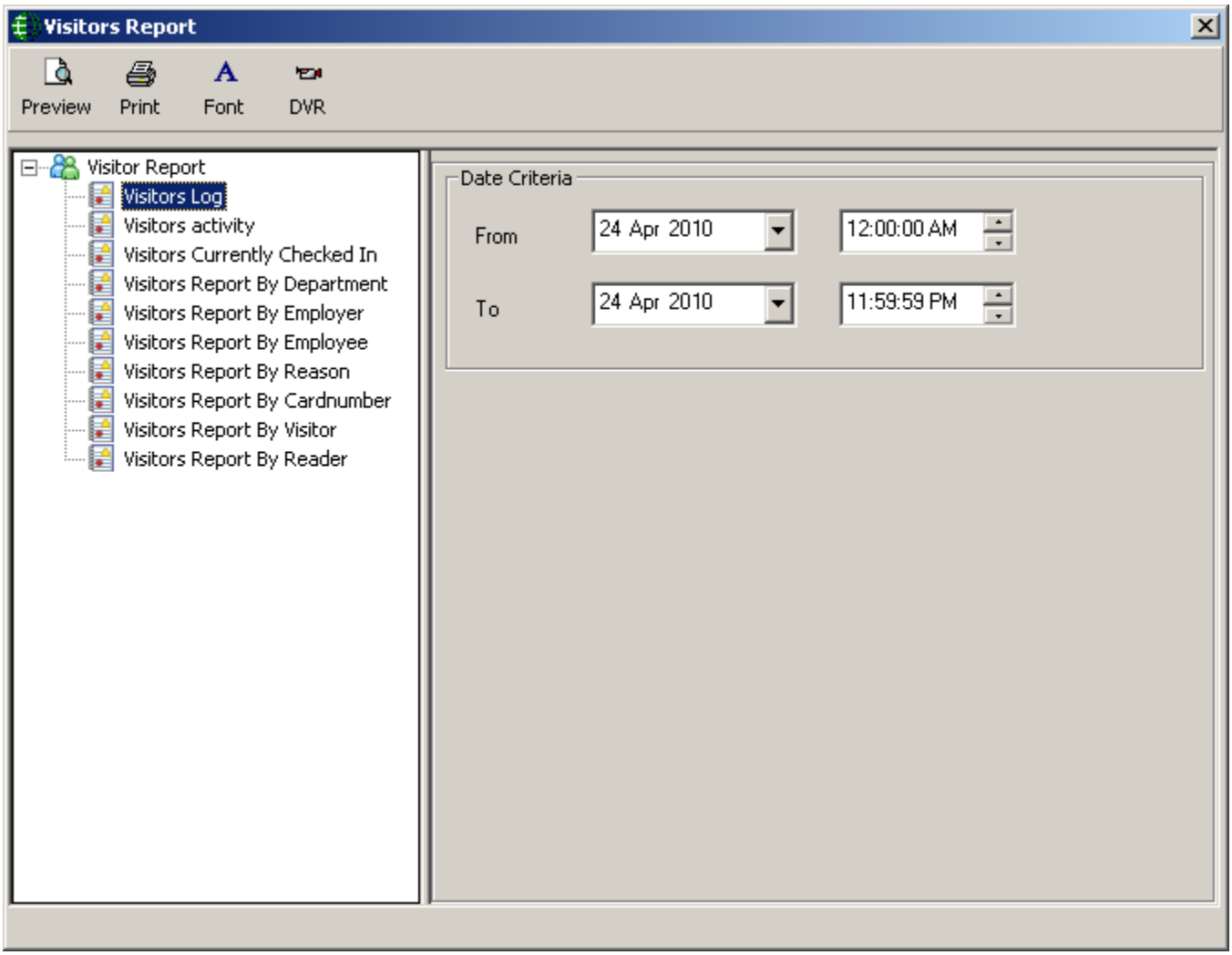
    - Use the *Move All*, *Forward*, and *Back* arrows to select sort fields.
    - Then choose *Ascending* or *Descending* for that field.
    - Click the *Next* button to go to next screen.

- Click on *Preview Report* to see the report or click on *Begin Again* to view a new report or click on *Finish* to end.

The user can follow similar steps to preview or print other kinds of *Database Reports* as well.

Visitor Reports[28]

Select *Visitor Reports* from the *Reports* menu to launch the following window, where the user has the option of selecting from many available visitor report formats.



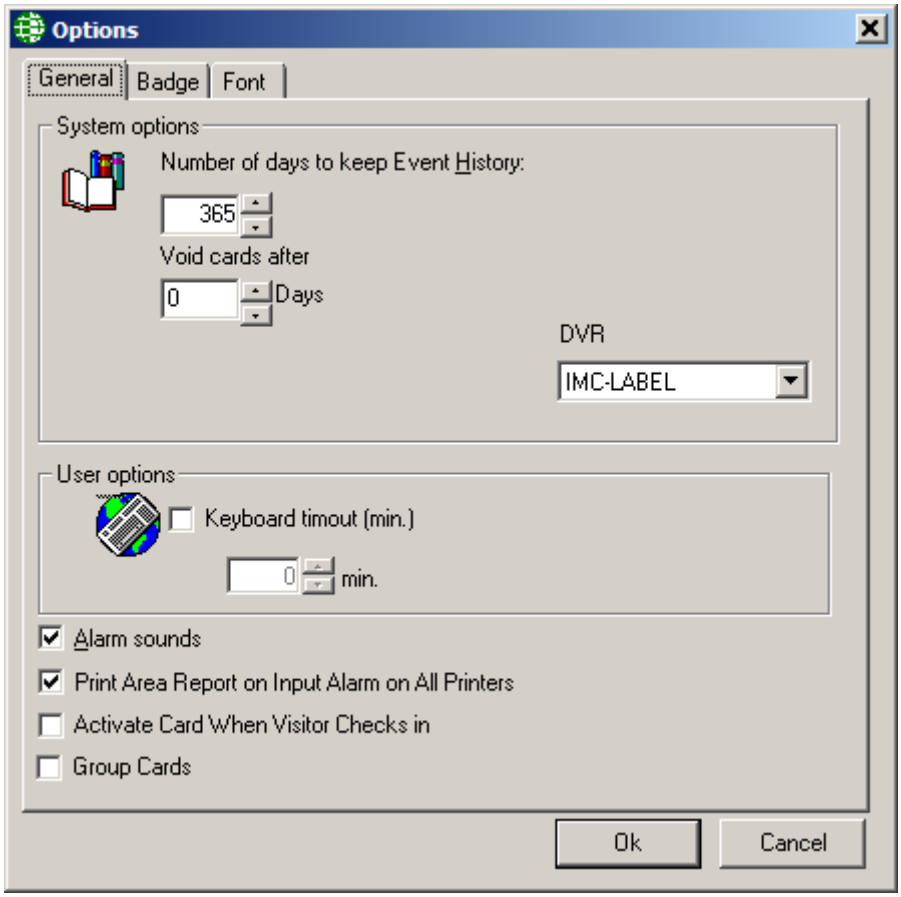
Choose a report format and select the *Start* and *End*, *Date* and *Time* for the time period you want to preview the report for.

[28] This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

Chapter 9
Options

System Options

General



System Options

Number of days to keep Event History

The *System Options* window allows the user to customize number of days to keep *Event History* and *Keyboard* time-out in minutes. The default "number of days" to keep *Event History* is 365 days. Each history file keeps the history information of one calendar day. If 365 days of history is being kept then only 365 files will be kept. When a new history file is created, the oldest file will be deleted so that only 365 files are maintained.

Auto void cards after:

At 1:00 am cards that have not been used within the specified number of days will be automatically deactivated. No cards will be deactivated if the number of days is set to zero.

DVR[29]

The DVR box allows the choose one of the two options available for video display: IMC-HISTORY or IMC-LABEL. IMC-LABEL displays the camera label on the played back history from the DVR.

User Options

If a user has entered a keyboard time-out, Integra32™ will automatically log-out if there is no mouse or keyboard activity for the duration of keyboard time-out period.

To prevent auto log-out, *click* and uncheck the keyboard time-out option.

Alarm sounds

Click in the check box to turn on the alarm sounds, which are heard through the computer speaker. (*Click again in the check box to turn it off*.)

Print Area Report on Input Alarm on All Printers

Click in the check box to turn on the feature (*click again in the check box to turn it off*). With this box checked all prints listed on the server will print an area report when the input goes into alarm. If the box is not checked the report is printed only on the default printer of the server. An input must be selected in the area properties before any report can be printed.

Activate Card When Visitor Checks In

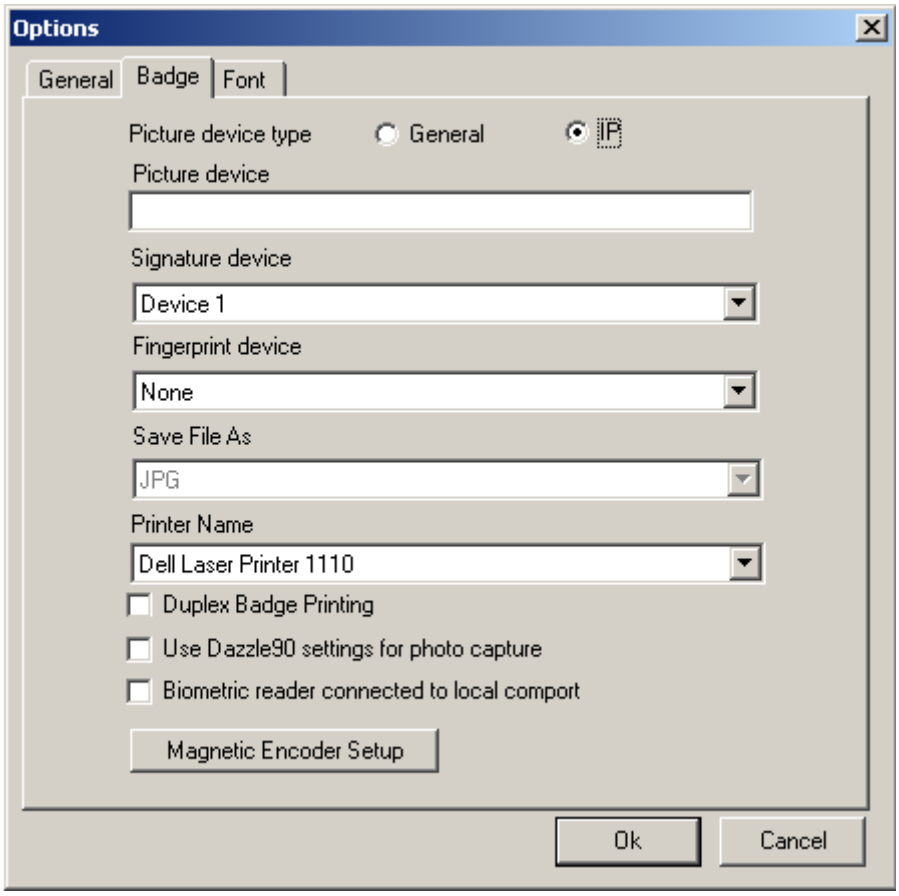
With this box checked a visitor's card will be activated when the visitor is 'checked in' and deactivated when the visitor is 'checked out'.

Group Cards

This selection tells the system that cards under a single cardholder are to be grouped, so that if one of these cards is used to enter an area, all of the cards in the group will not be allowed to be used to go into the same area. Any one of the cards may be used to go into another area. For this feature to work *PC Decision Required* and *Hard Antipassback* must be on.

[29] This selection is only available if the optional license for the DVR Software has been purchased and installed.

Badge[30]



Use this tab to define properties of the Badging utilities. Designate where the cardholder's image, signature, and fingerprint will be acquired. For devices to be listed here they must first be installed in the operating system according to the requirements of Badges. They must also be Twain devices. IP cameras can be selected as well.

Designate as well the format to save the image as and what printer to use for printing badges.

☑ Also click in the check box for double sided printing of badges.

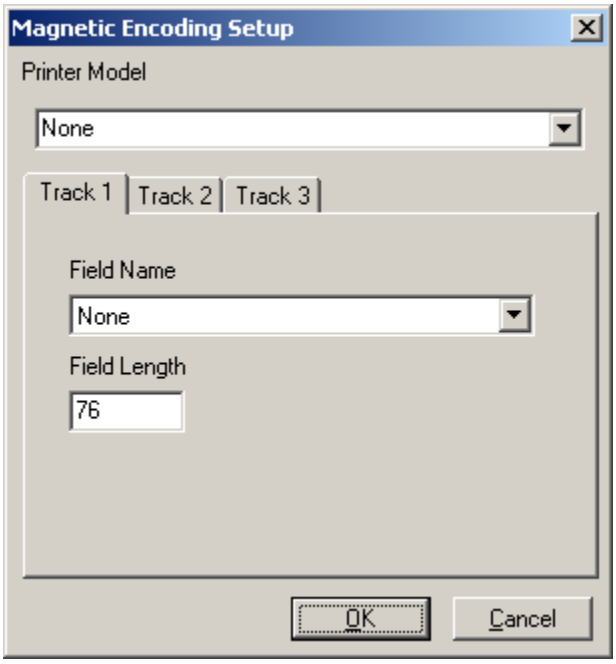
☑ Check 'Use Dazzle 90' if you are using a Dazzle 90 for photo capture.

☑ If you are connecting Biometric Readers to your COM port check the box.

[30] This selection is only available if the optional license for the Badging Software has been purchased and installed.

Magnetic Encoder Setup

Clicking in the *Magnetic Encoder Setup* button under the *Badge* tab of *System Options* window will launch the following window to setup properties for magnetic encoding.



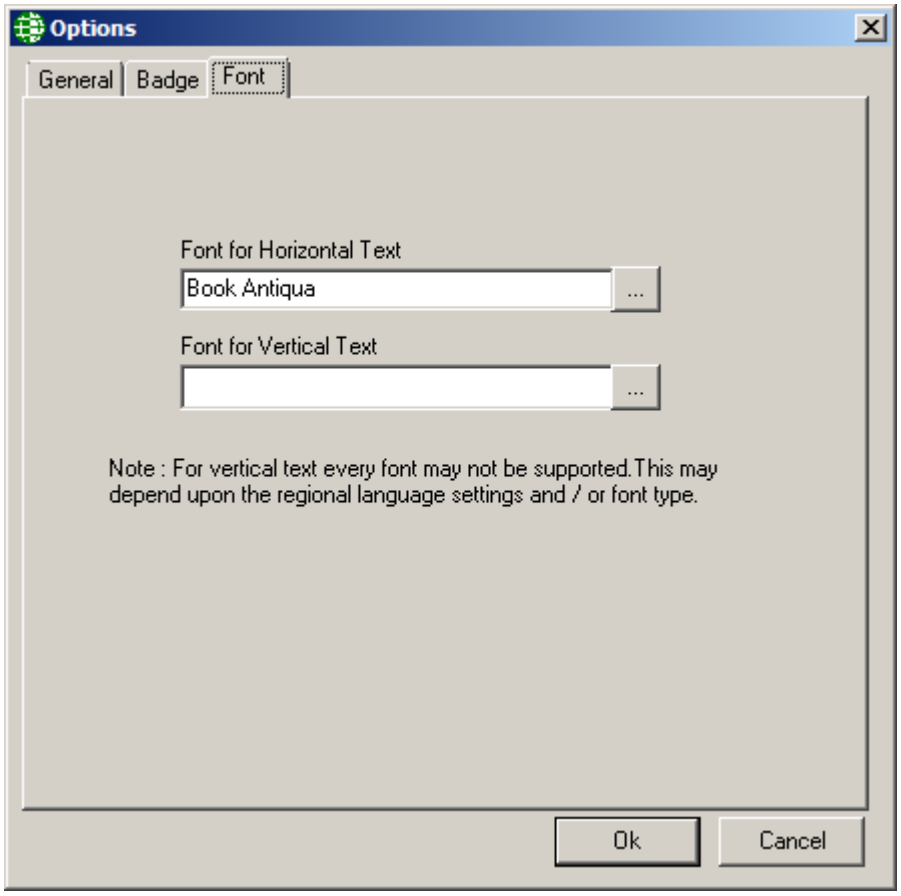
Select the printer model in this window. The fields to encode can be selected for each track once the printer model is selected.

Note:

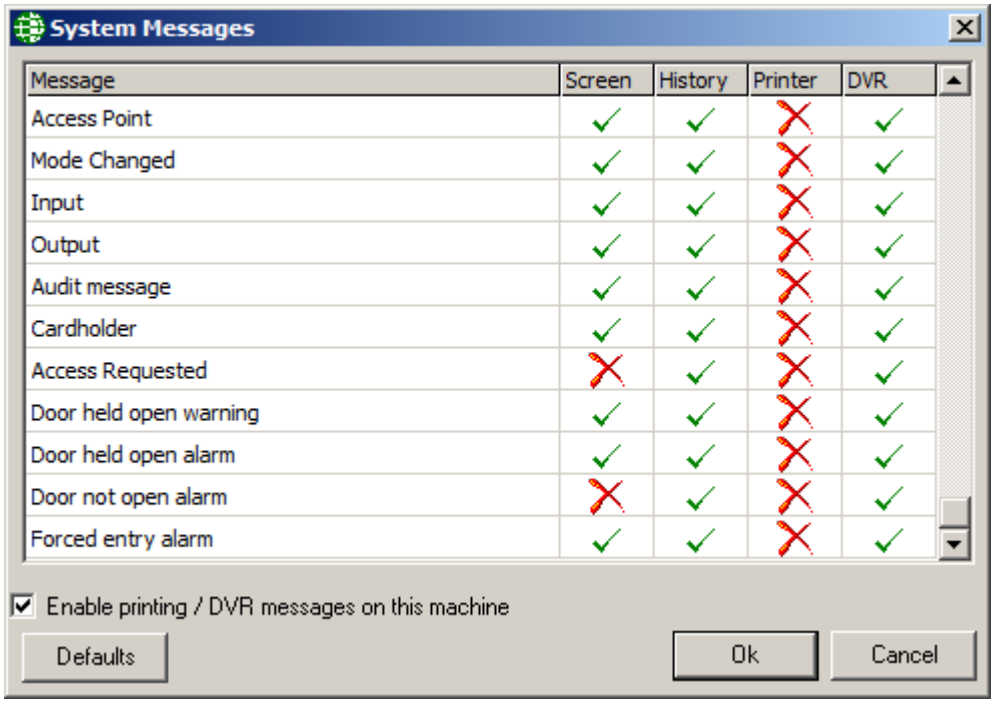
- The field length is fixed and cannot be changed.
- If *None* is selected for the printer model, the track fields for encoding will not be available.
- The printer properties for encoding should be setup for the printer from the control panel.

Font

You can change the default font for the main client screen by browsing the font list, select a font, and click OK. The default font is MS San Serif.



System Messages



The user can customize how the system handles messages. (*E.g. If the user doesn't want a particular message to appear on screen, like the Access Requested message, it can easily be turned off with a simple click. Simply change between 'Yes* ✓ *' and 'No* ✗ *', to stop the display of selected messages on the screen or from being sent to history*.) The user can also send messages to a printer (*selectable by message*).

Messages can also be sent to ASCII ports or a DVR. DVR configuration will be required for this to function correctly. Check the box if the DVR or printer are on the local machine.

Access Point Activity

The Access Point Activity feature can be used with a CCTV system for video verification. To do this enable PC Decision in the *Modes* tab of the *Access Point's Properties* window and check Access Point Activity – Access Requested in the *Advanced* tab of the *Access point's properties* window. Now whenever a valid card is read at the access point the Access Point Activity window will open displaying the cardholder's picture, name, and card number, the date/time of the event and at which reader the event happened.

If PC Decision is not used in the *Modes* tab then the Access Point Activity window will show all access granted and/or access denied events that occur at selected access points.

Grant Access
Grant access will grant access at the reader currently shown in the *Reader* box of the *Access Point Activity* window.

More/Less

The *More* button will add a section to the bottom of the window that will display the contents of the cardholder's notes tab. Information about the cardholder that needs to be readily available can be display this way. The *Less* button will remove this extension.

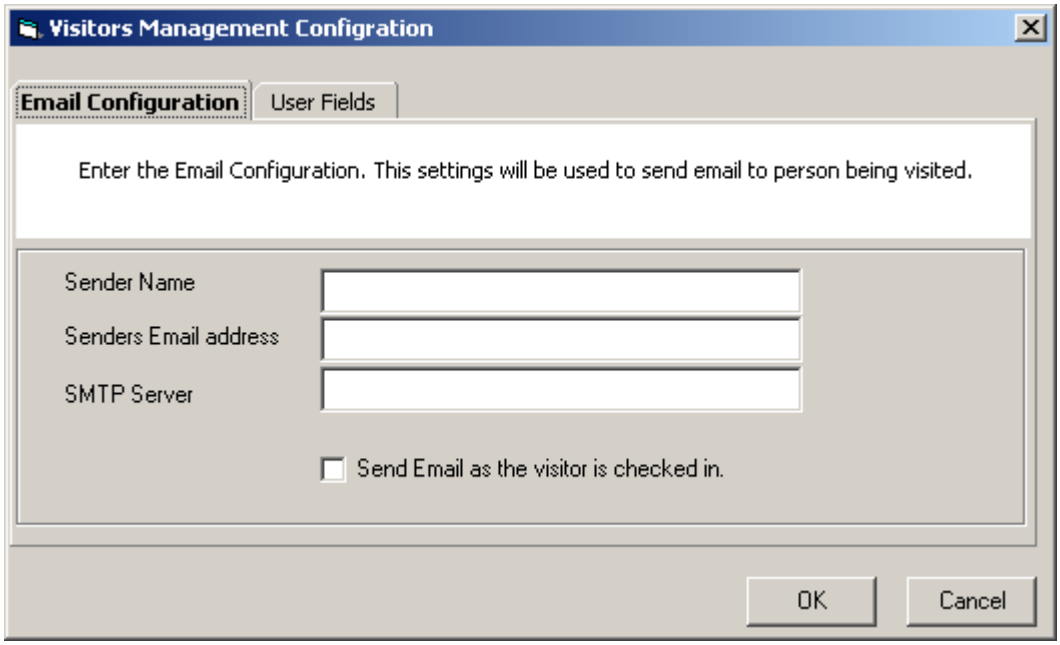
Hide

The *Hide* button will remove the Access Point Activity window from view without turning it off. You can also minimize this window. The difference between hiding and minimizing is that a hidden window won't show up on the task bar.

VM Configuration[31]

eMail Configuration

To send emails to cardholders announcing their visitors you need to configure the sender's email information on the screen depicted below.

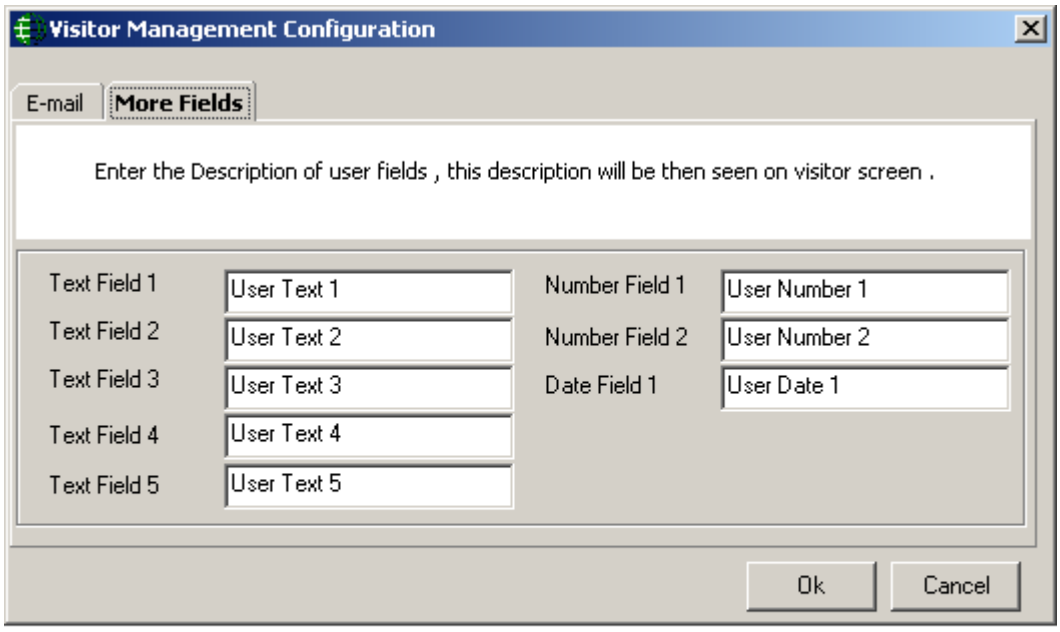


The *Sender Name* is used to let the cardholder know where the visitor is, or entering from. A site may have more than one entrance that visitors can come in by and the cardholder being visited may need to know where the visitor is.

☑ Check the box 'Send Email as the visitor is checked in' to have an email sent automatically to the being visited cardholder. The being visited cardholder's Profile Tab must have an email address entered for this feature to work.

[31] This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

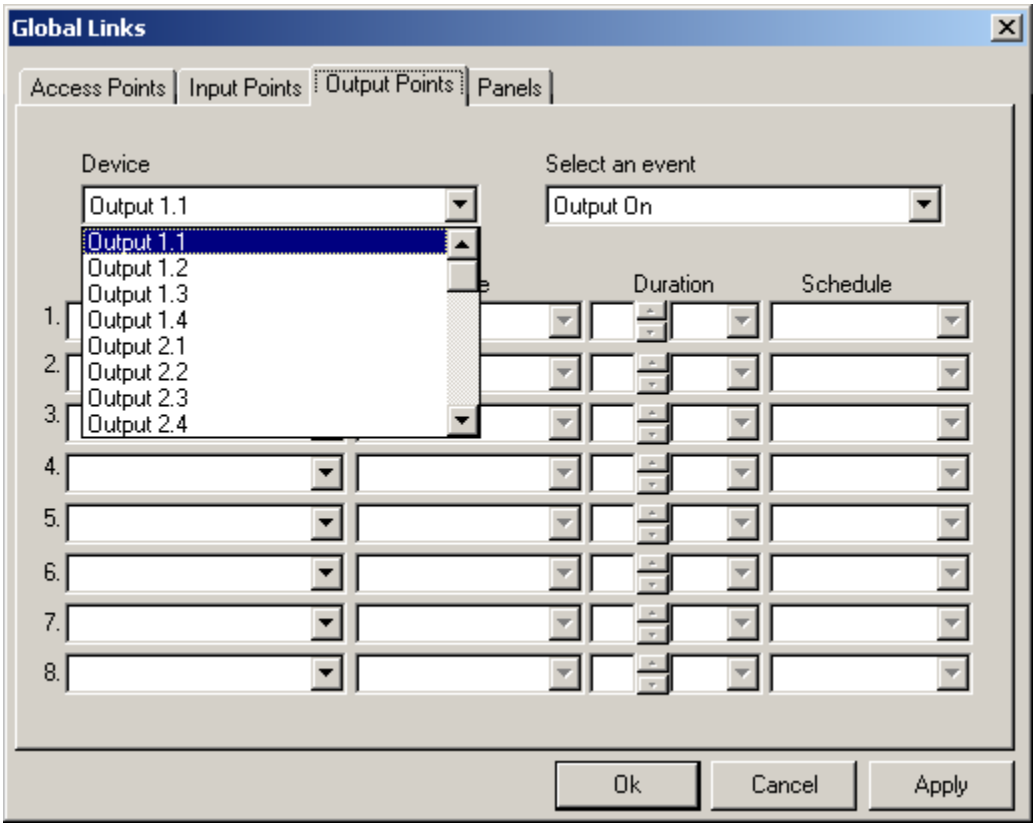
User Fields



Define the name of the fields for entering data under the *User Fields* tabs of *Visitor*. Use this to customize the visitor data saved in your system.

Chapter 10
Links

Global Links



Global Links like Global APB require the interaction of the PC. These links cannot be executed if the PC is not online. As with local links you choose which event on what device will cause the link to be executed. Then you can choose up to eight things to have happen. These links can be executed on any panel in the system.

Details on programming links can be found in Chapter 5 under Access Points, Inputs, and Outputs.

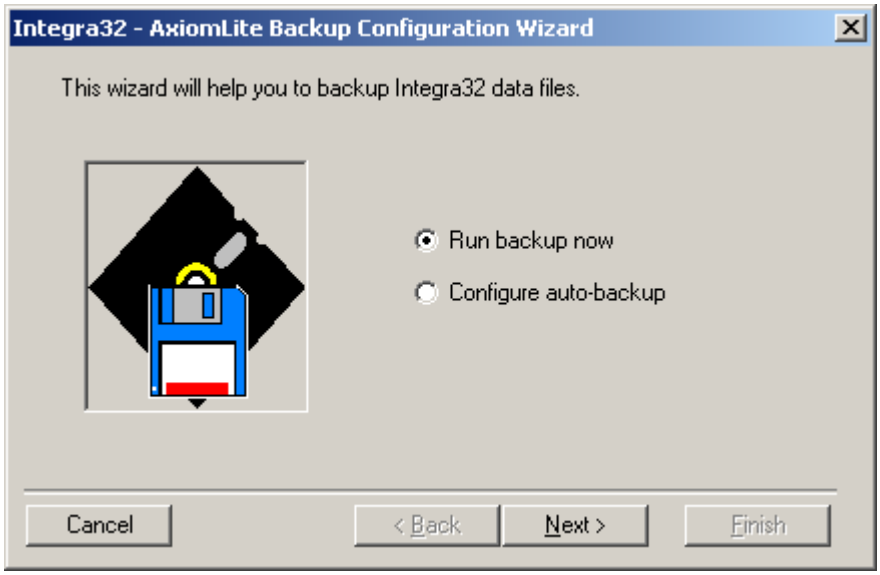
Chapter 11
Tools

Backup

The Integra32™ *Backup Configuration Wizard* is used to backup your data files. You can run the *Backup* immediately or configure the auto-backup to run at a later time.

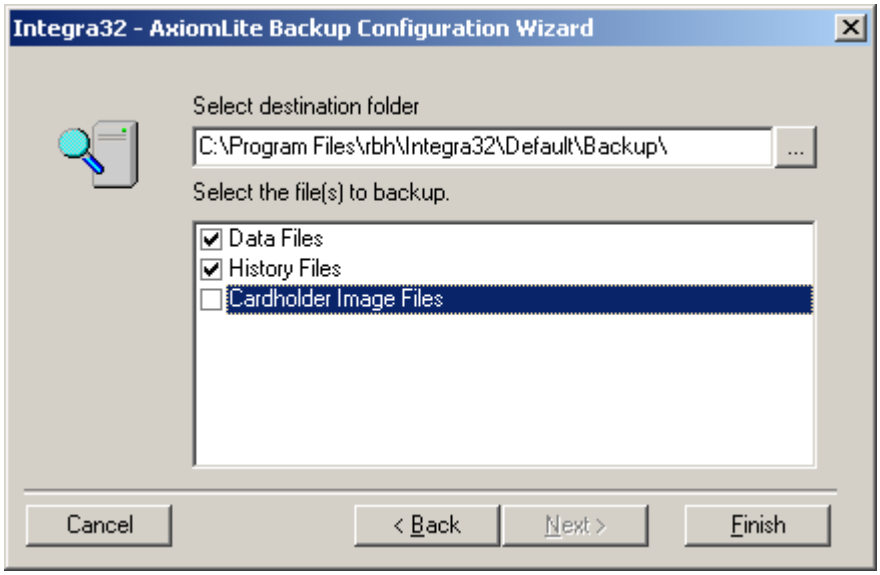
Your Operating System most likely will also have its own backup utility. It doesn't matter what method you use as long as you backup your files regularly.

["It's not a matter of if a hard drive fails, but when." *Unknown*]



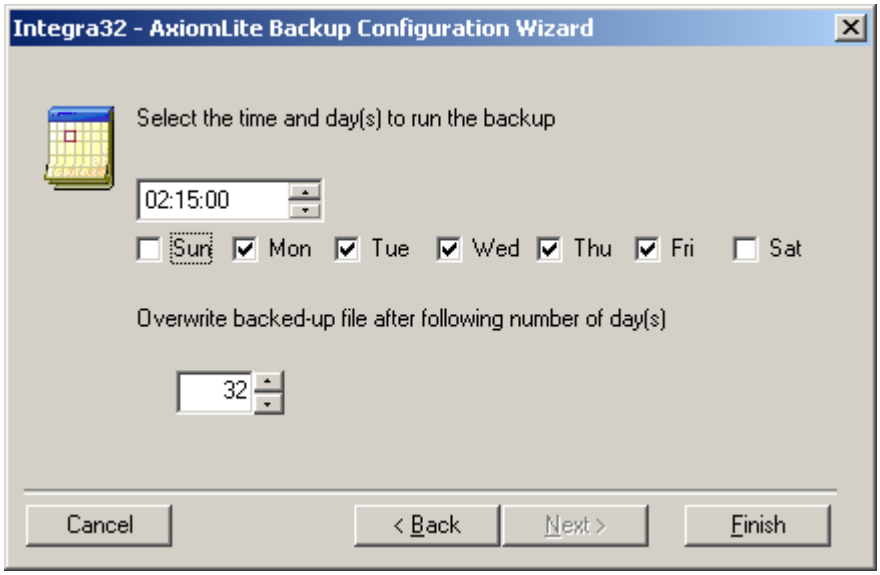
Run Backup Now

Run Backup Now option is used to run an immediate backup. Follow the wizard for this option. From the *Backup Configuration Screen* the destination folder into which the backup files will be saved is selected. (*The **default** destination setting is …\Integra32\Default\Backup*.) Checking *Data Files* will backup the data files (*particularly AxlogxLT.mdb, AxsystLT.mdb, & AxuserLT.mdb*). While checking *History Files* will backup all of the currently held history files. *Cardholder Image Files* when checked will backup the cardholder pictures. The *Log Screen* will display these files as they are backed-up.



Configure Auto-Backup

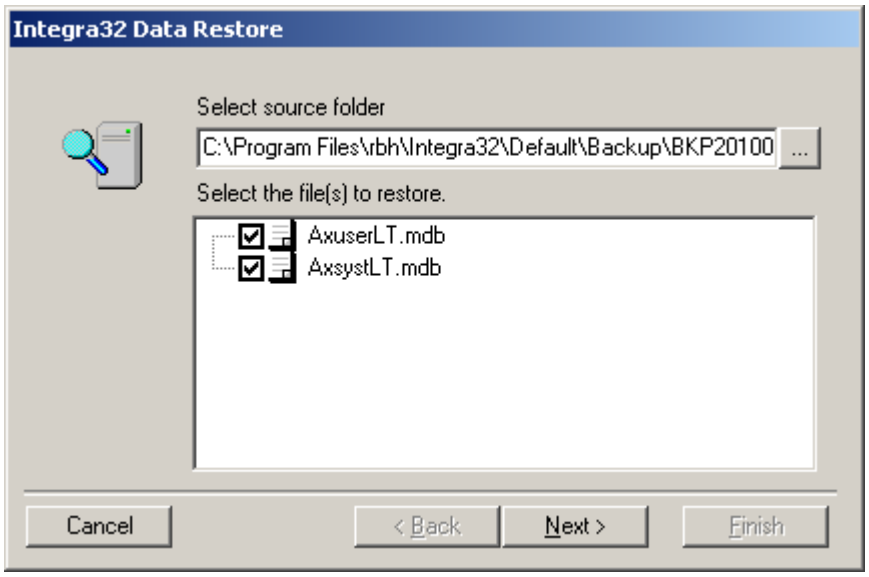
The auto-backup can be configured to happen at a specified time on specified days of the week. For example the backup can be performed at 11:30 a.m. every Monday, or at 10:15 p.m. every Tuesday and Thursday. These backed-up files are saved by date (*the file is designed* bkpYYYYMMDD *where YYYYMMDD is the backup date*), and you can set how long they are to be kept. If for example you set the backup for every Monday and Friday to be kept for 31 days. Backups older than 31 days will be over written.



Click *Finish* to allow the system to run the auto-backup at the specified day and time.

Restore

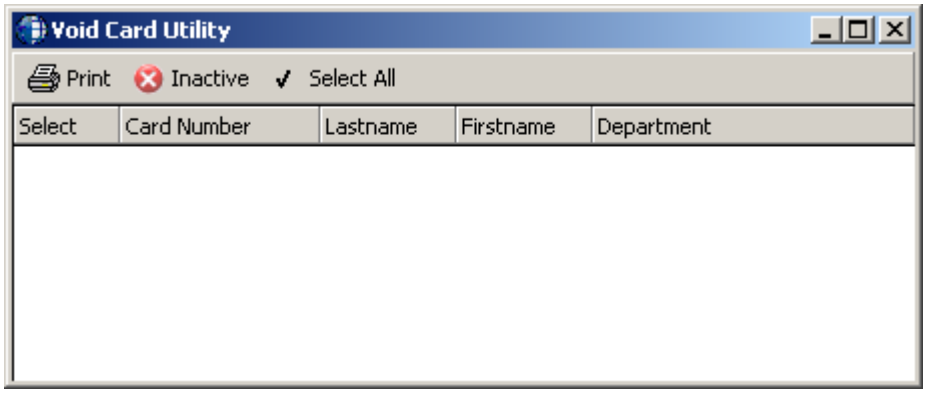
To restore backed-up files you must log into *Integra32 Data Restore*. *Integra32 Data Restore* is located under Programs > Integra32 Security System which is accessed by clicking *Start*. You will be required to login before getting to the *Data Restore Screen*.



The *Data Restore Screen* allows you to select which files are to be restored. You can even select which image files are to be restored.

Void Cards

From *Void Cards* the operator can manually void (deactivate) cards that have not been used for a preset number of days. The number of days is set under Options – System Options.

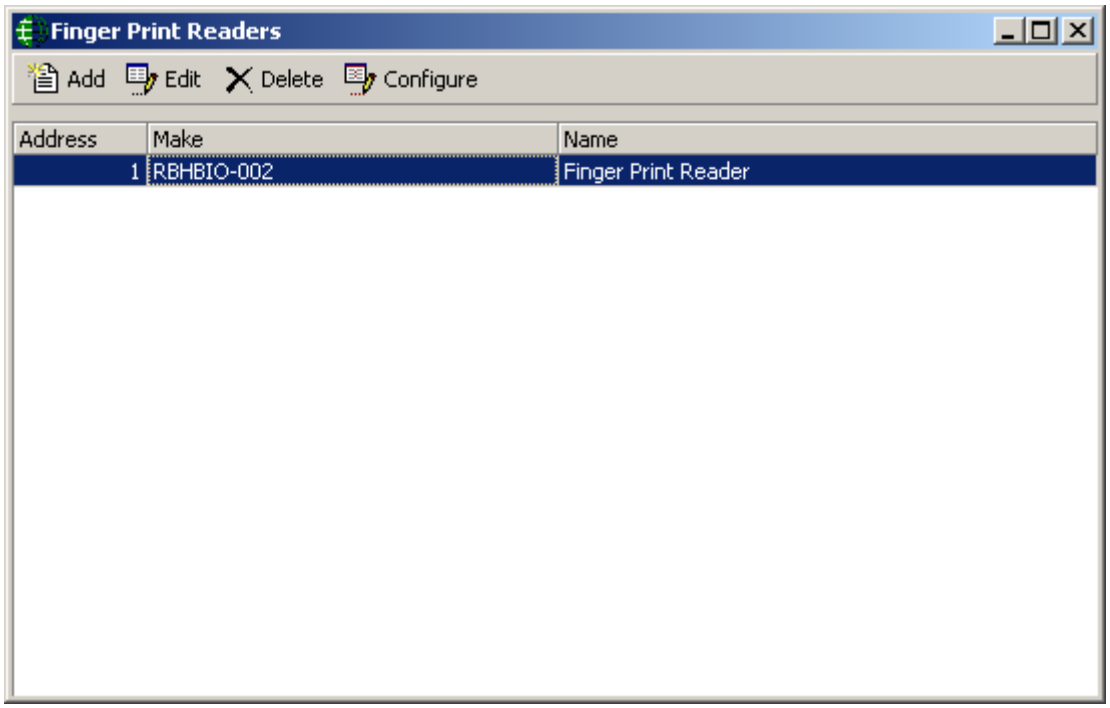


Print *will produce a hard copy of the cardholders listed at the time* Print *is selected.*

Void will immediately deactivate all selected cards.

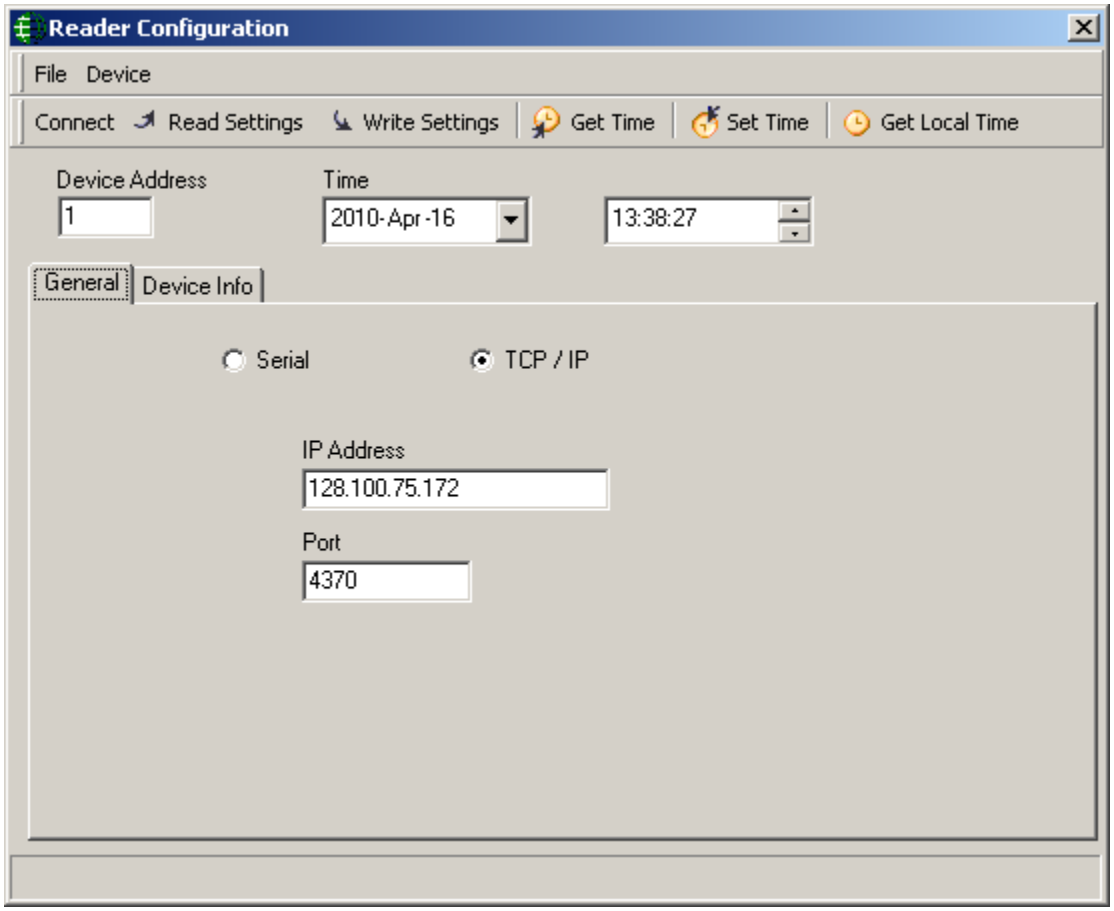
Select All will put a check mark in the select field for all of the listed cards.

Finger Print[32]

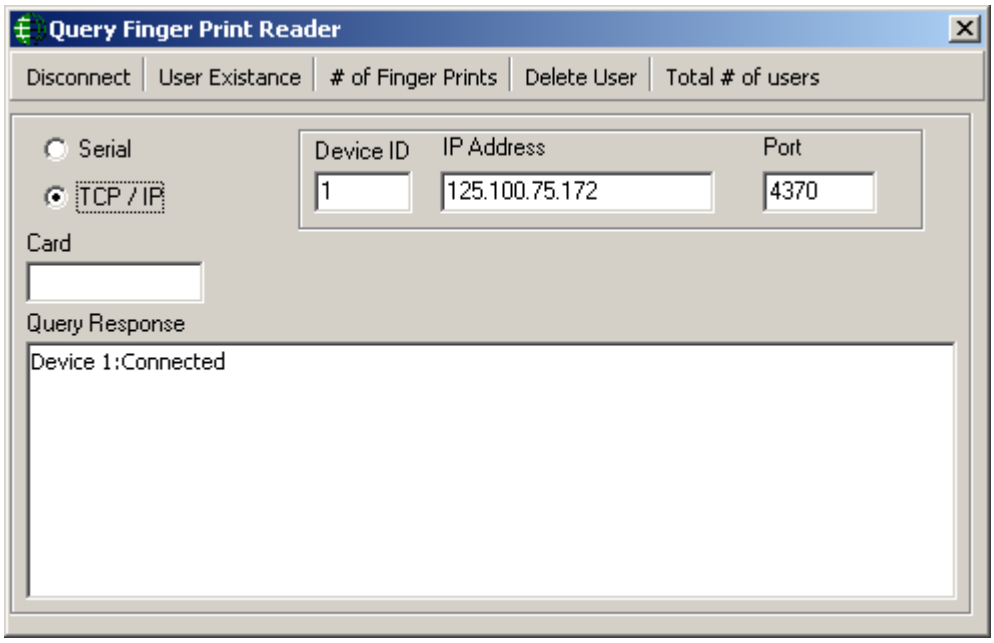


Finger Print opens a screen from which to manage the RBHBIO-002 and their finger print data.

[32] This selection is only available if the optional license for the Finger Print Reader has been purchased and installed.


Reader Configuration
File Device
Connect Read Settings Write Settings Get Time Set Time Get Local Time
Device Address
1
Time
2010-Apr-16
13:38:27
General
Device Info
Serial
TCP / IP
IP Address
128.100.75.172
Port
4370

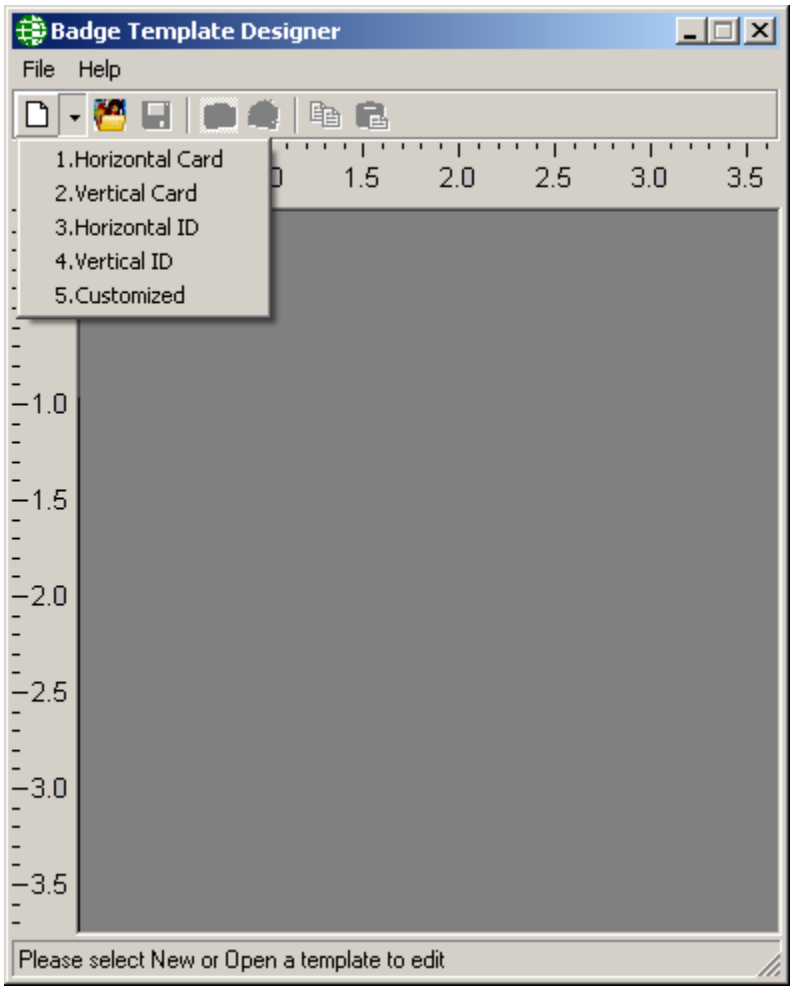
Query Finger Print Reader[33]



Use this selection to query RBHBIO-002 readers.

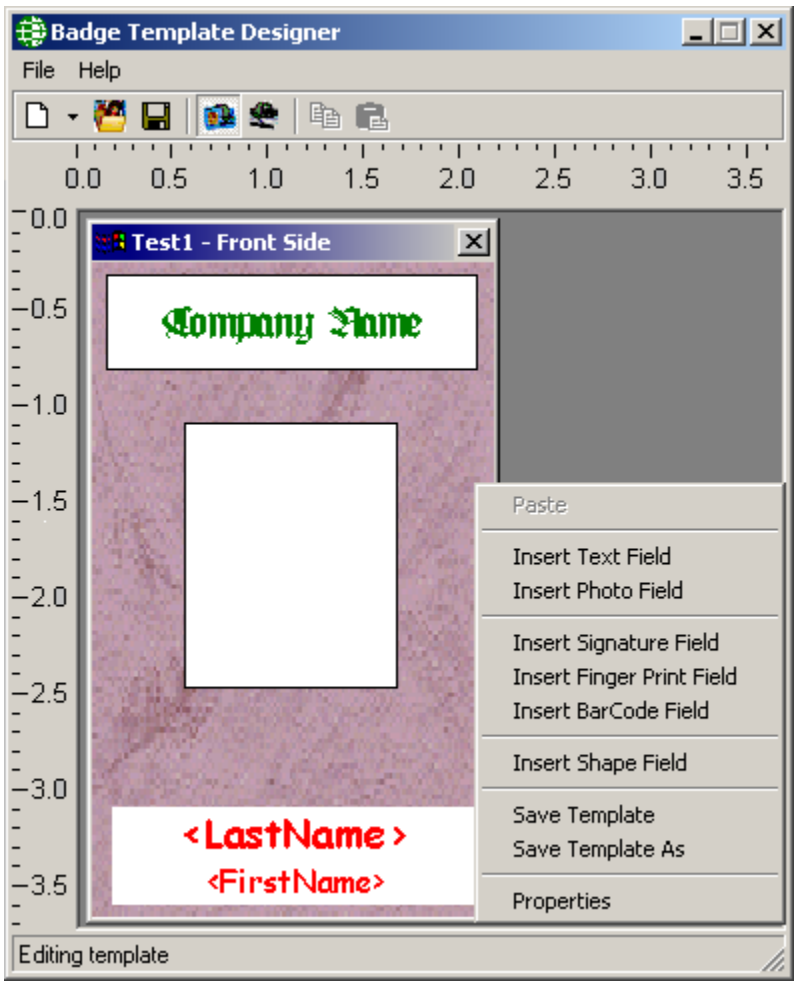
[33] This selection is only available if the optional license for the Finger Print Reader has been purchased and installed.

Badge Template Designer[34]



The Badge Template Designer can create standard or customized badge sizes. Select one of the five options available from the *Create a new template button* of the toolbar Templates can be saved and re-opened.

[34] This selection is only available if the optional license for the Badging Software has been purchased and installed.



Right clicking on the badge will bring up a menu list. From here you can add a text, photo, fingerprint, signature, or barcode field.

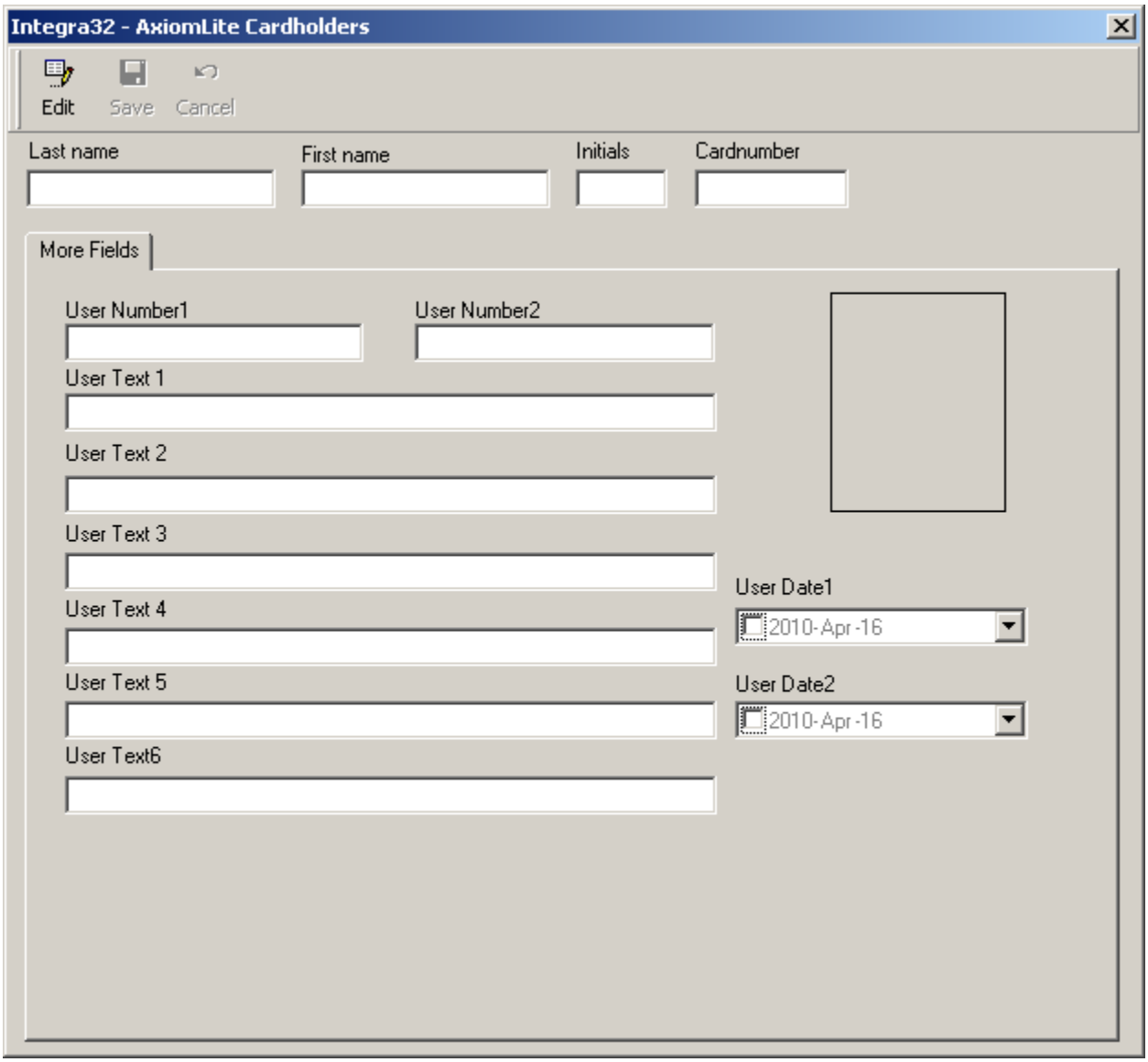
- Text fields can be static (*type in your own information*) or it can get data from a field in the database (*e.g. name or card number*).
- Photo fields can also be *static* (*so that you can insert your own picture or logo*) or *picture field* where you can display the cardholder's image that is stored in the database or acquire the picture of the cardholder if a camera is installed on your computer.
- Fingerprint fields[35] can be added to the badge.
- Signature fields[36] can be added to the badge.
- Barcode fields[37] can be added to the badge.
- A shape field can also be added to enhance your badge.
- In the properties of the badge you can set the background colour of the badge, you can also add a background picture.
    - You can right click on a field to modify its properties or to delete it.

[35] To use these options you may need optional hardware devices.

[36] To use these options you may need optional hardware devices.

[37] To use the Barcode field, you need to install barcode fonts in your control panel, which are available in the *fonts\ Resources* folder of your Integra CD.

Card Custom Fields



Double click on a header while in the Edit Mode to change the name of the user field. This change will be shown in the *More Fields* tab of every cardholder

Card Import[38]

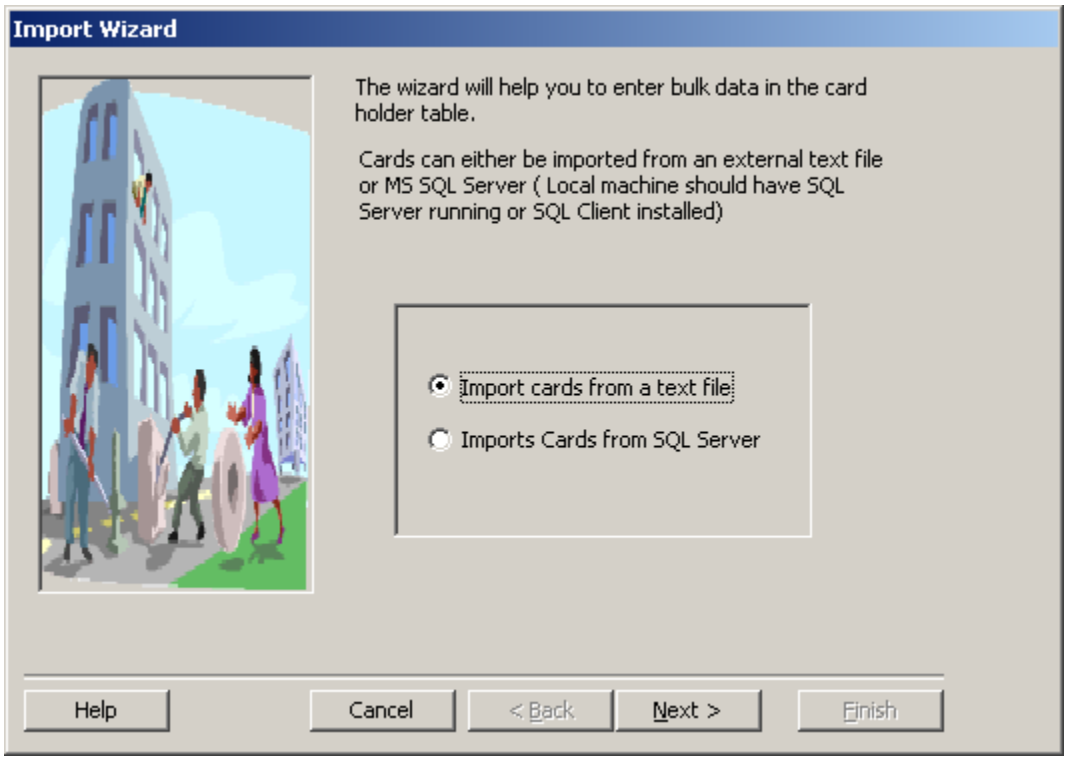
Configure Import Utility

The *Integra32™ Card Import Utility* is used to import cards and cardholder data from a text file into your Integra32™ database.

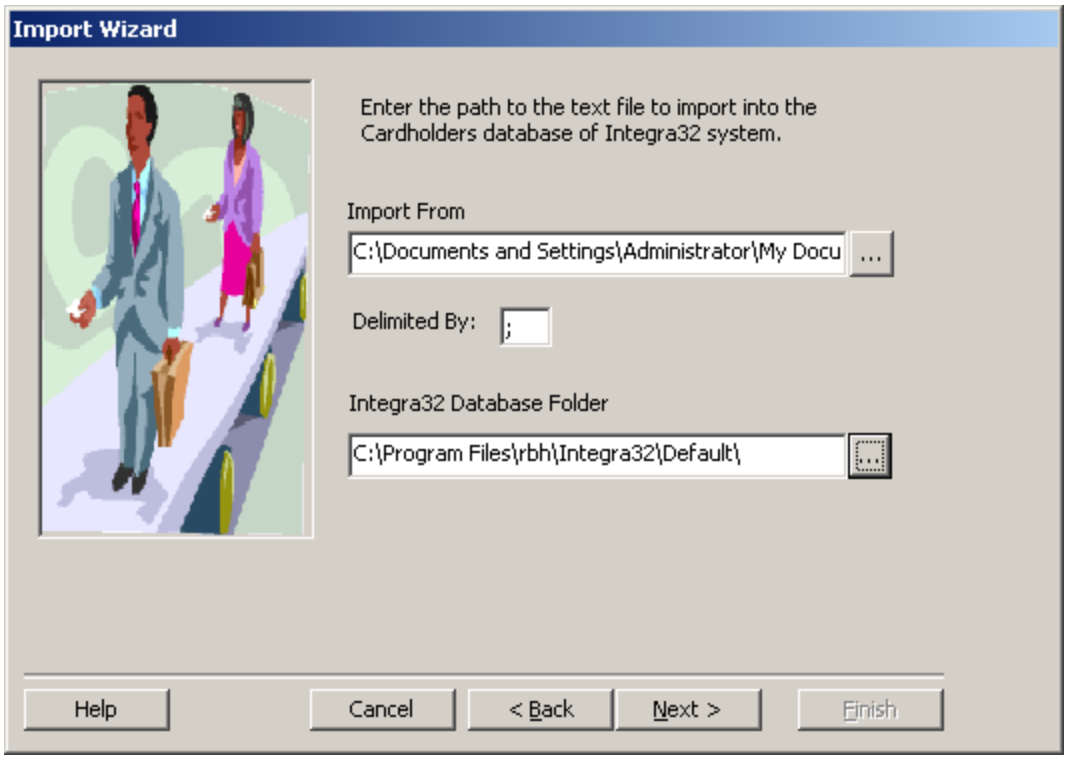
Select *Config Import Utility* to setup the import parameters.

[38] This selection is only available if the optional license for the Card Import Utility has been purchased and installed.

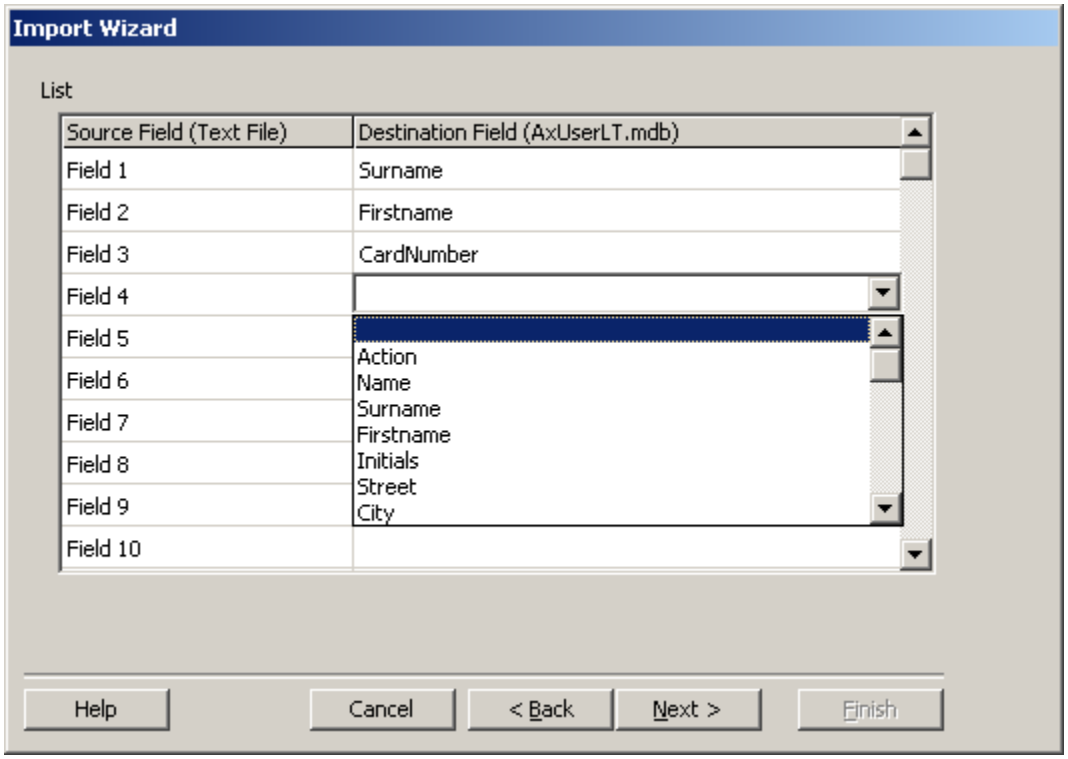
Import from a text file



Enter the source and destination paths as well as the delimiting character. Click *Next*.

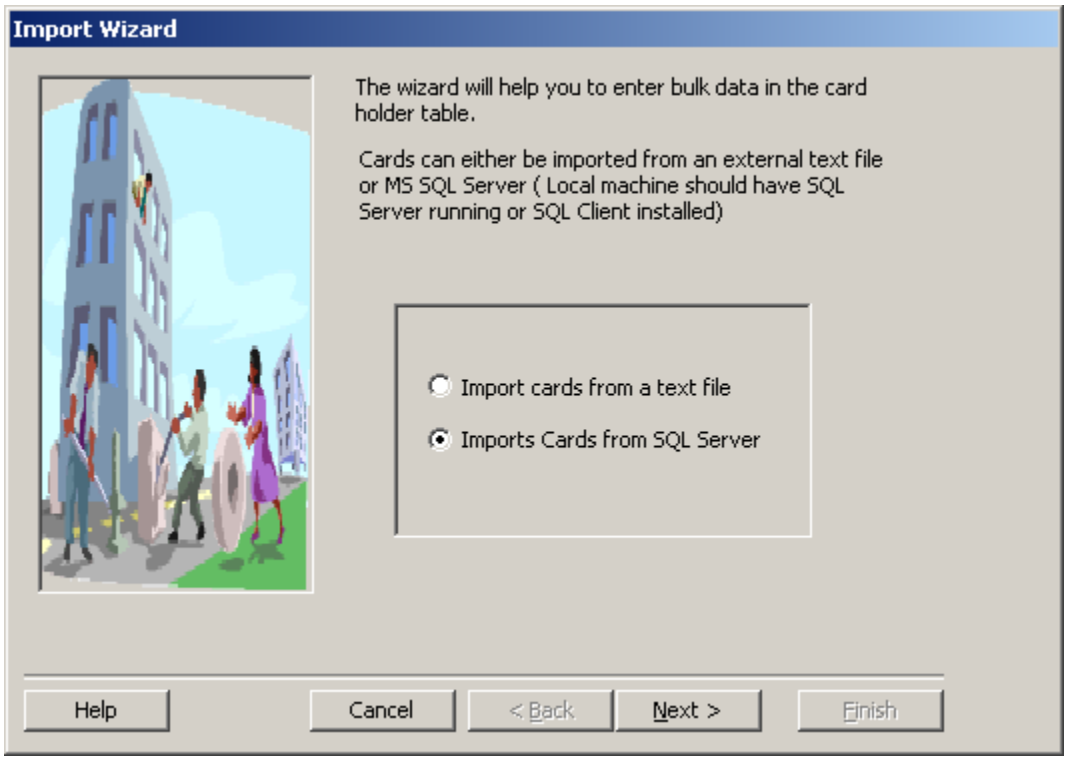


Then select the appropriate destination fields for the corresponding source fields (e.g. select *Surname* for *Field 1* and *Firstname* for *Field 2*) depending on the data in the text file.

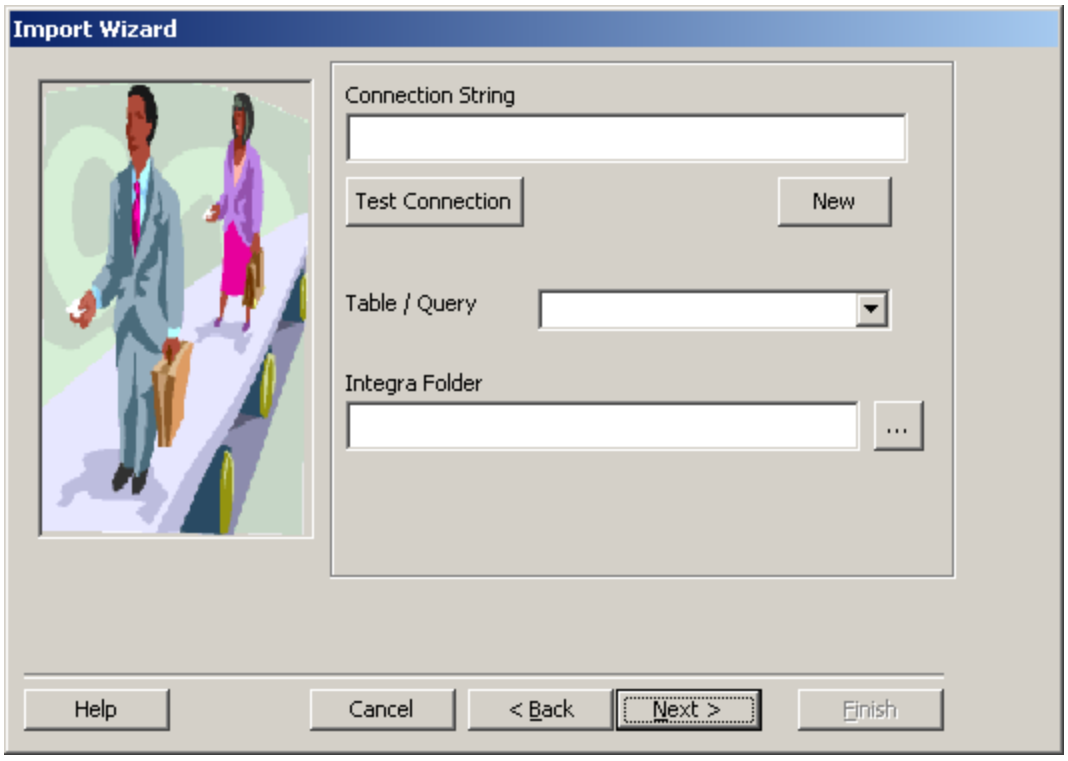


Click *Next* to continue.

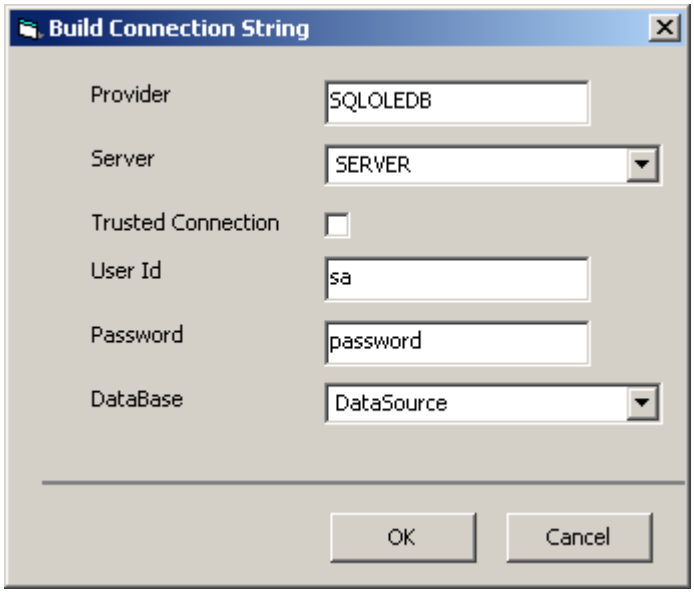
Import from a SQL file



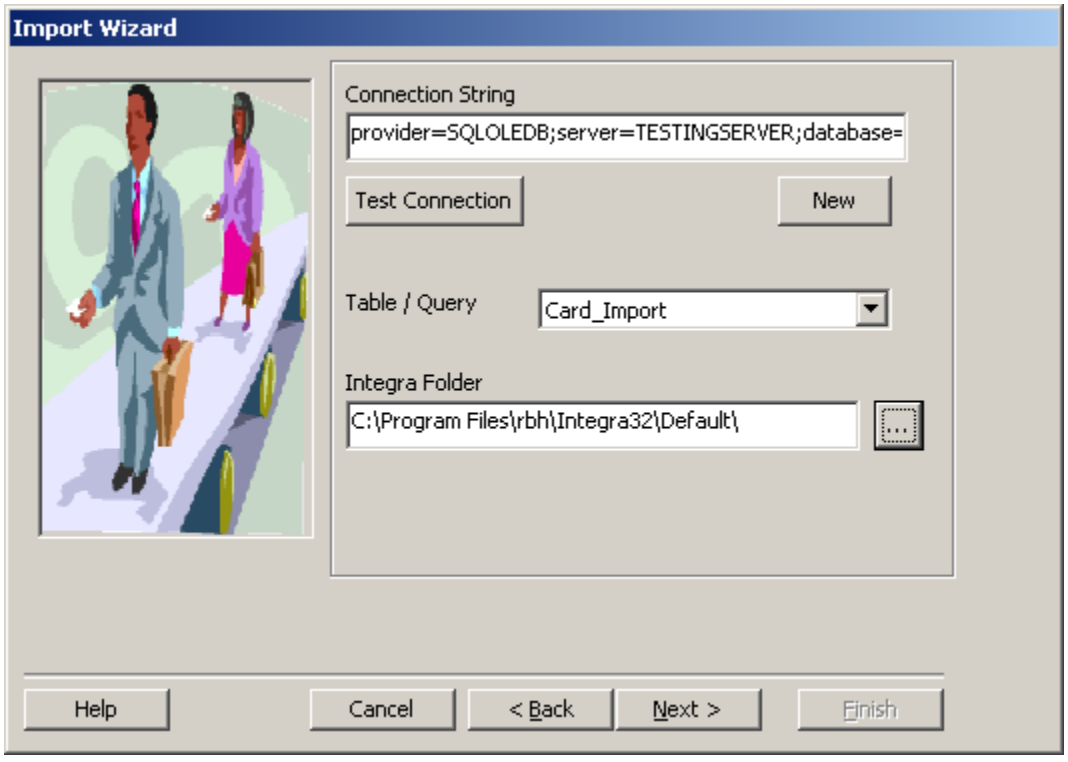
Click *New* to input the connection string.



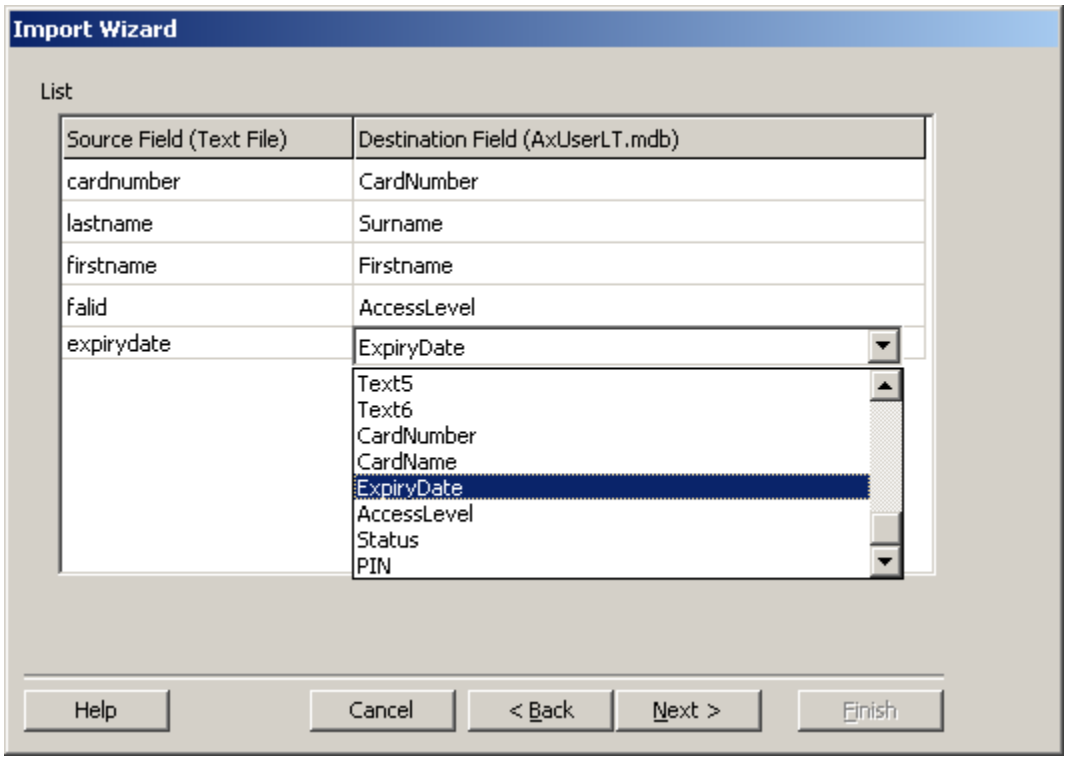
Use the pull-down to select the server. Enter the User Id and password. Then select the specific database on the server that holds the source data. Click *OK*.



You can verify the connection with Test Connection. Select the table or query of the database set above, and then provide the path to the target folder (by either typing or browsing).



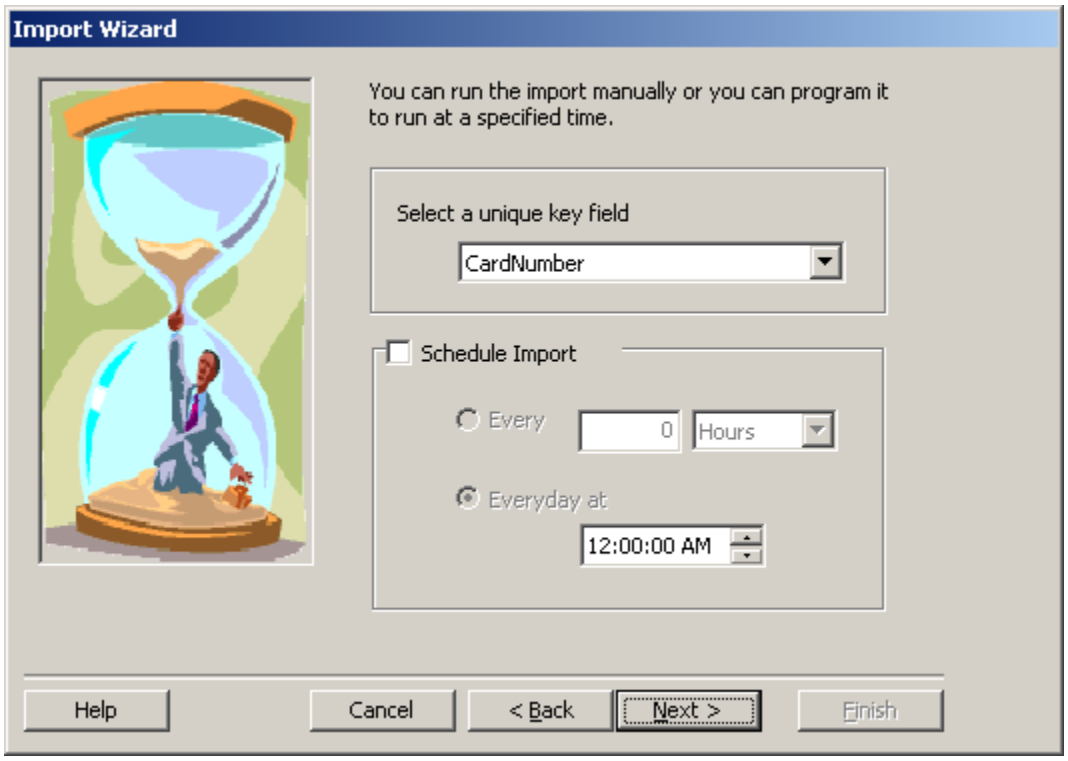
Then select the appropriate destination fields for the corresponding source fields (e.g. select *Surname* for *lastname*, *Firstname* for *firstname*, and *AccessLevel* for *falid*) depending on the data provided by the table or query.



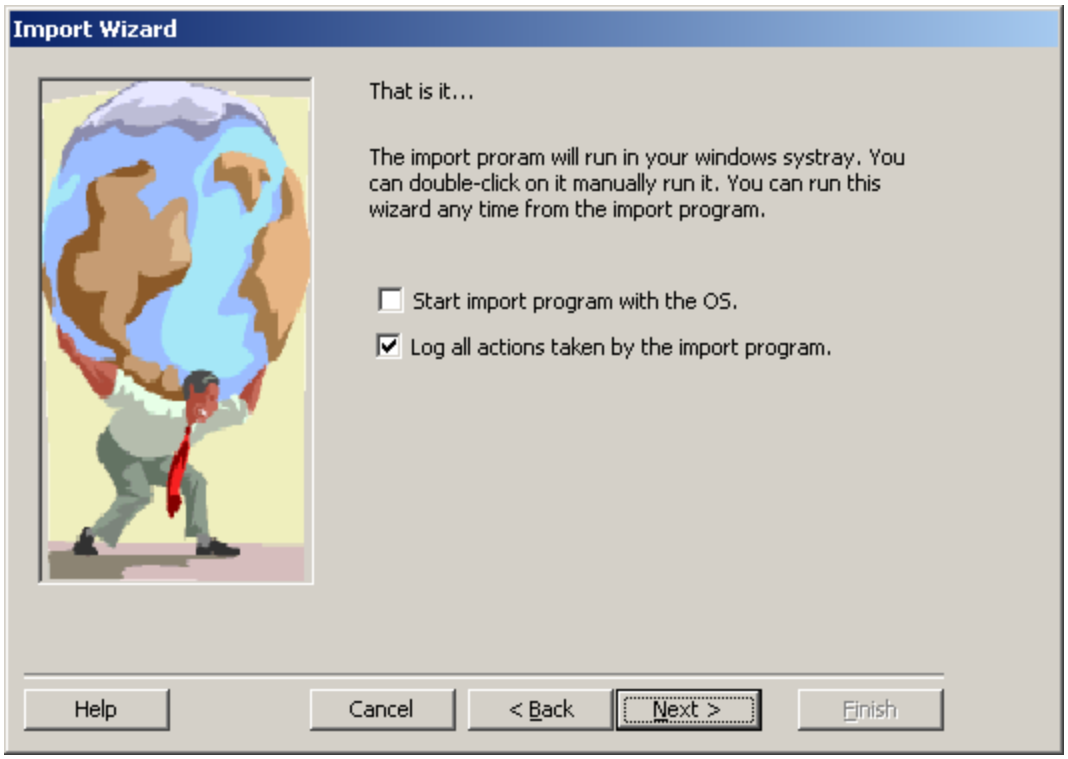
Click *Next* to continue.

Complete the configuration.

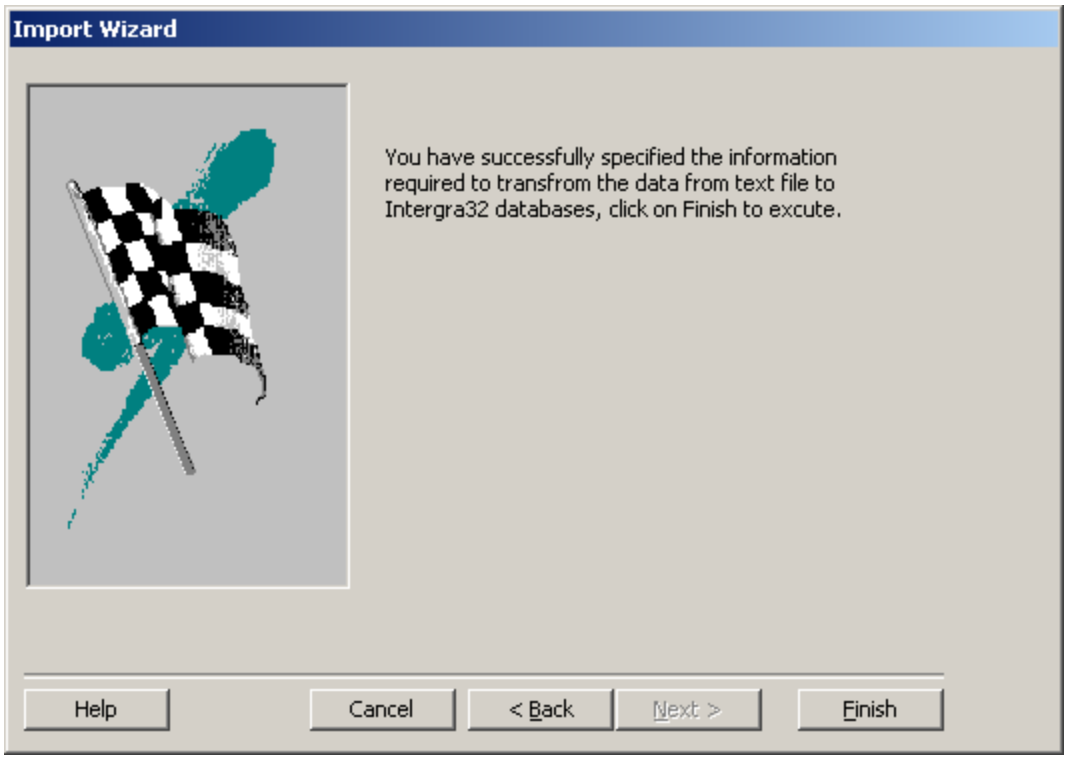
Select a unique key field. If required check Schedule Import and select either ‘every x hours or minutes’ or ‘everyday at x’.



Check the appropriate box to have the import utility start automatically with the Operating System. To have all actions taken by the import utility logged check the second box.



Note the icon in the windows *systray* indicating that the utility is active.



Click *Finish* to complete the setup. The utility can them run on a schedule or opened to be run manually.

Run Import Utility

Run Import Utility will run the utility immediately.

The status bar will display the progress and indicate when the import is complete.

View Log File

View Log File will call up Mimport.log a Notepad file. This file will show when the import started and ended, as well as any errors that occurred.

Chapter 12
Program Groups

Integra32™ Security System

Insure that the Integra32™ system is not running before making a selection here in the '*Program Groups*'. All selections here made will bring up the login window as shown in Chapter 2 on page 4.

Integra32™ Data Restore

Data Restore is described at the end of Chapter 10.

Integra32™ Database Maintenance

Running the '*Database Maintenance*' will compact and repair the Integra32™ databases. The '*Repair*' will correct most corruptions in the databases. Those that can't be repaired will produce an error message.

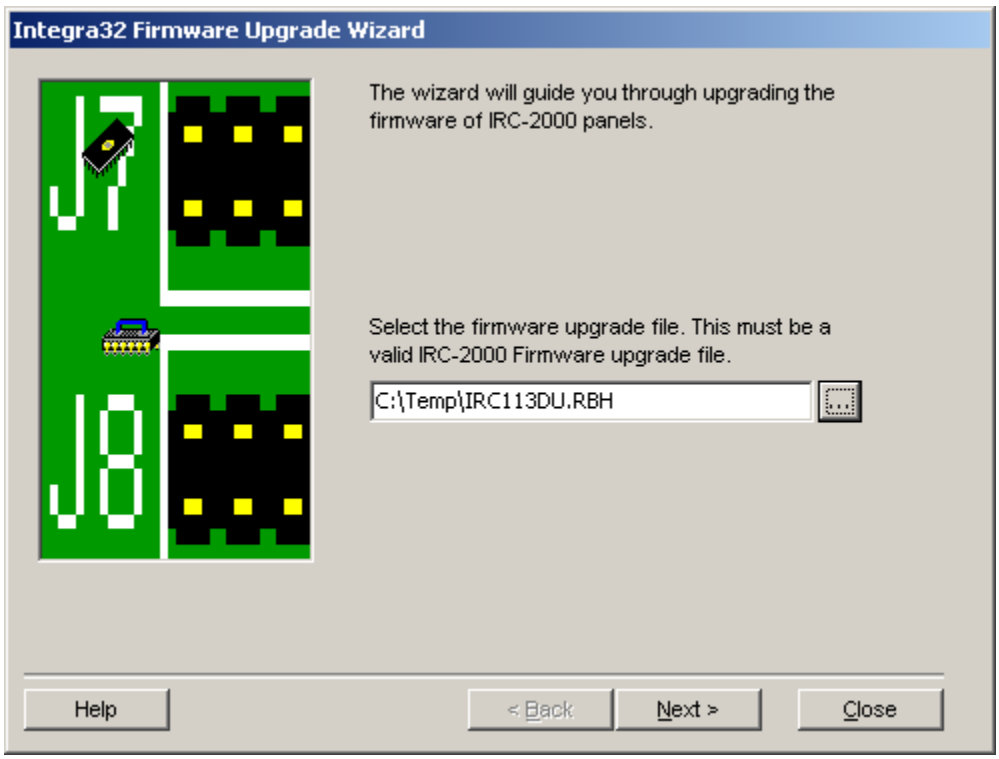
Integra32™ Firmware Upgrade

Before Upgrading

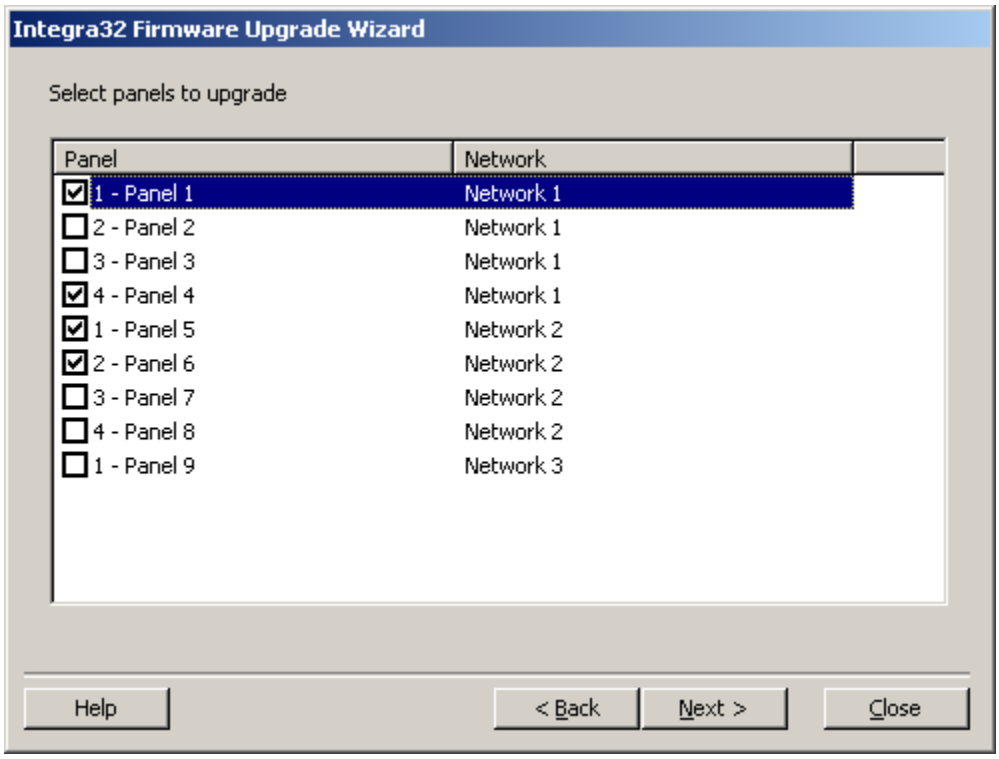
1. Before starting the firmware upgrade be sure to know where the upgrade file (**.rbh*) is located.
2. Although upgrading will not affect the panel's memory, it is recommended that you download all files to the panel after upgrading to ensure that any new features are properly installed.

Upgrading

After logging in the Upgrade Wizard will come up. Browse and select the upgrade file (**.rbh*). The upgrade file's path will be shown in the box next to the browse button.

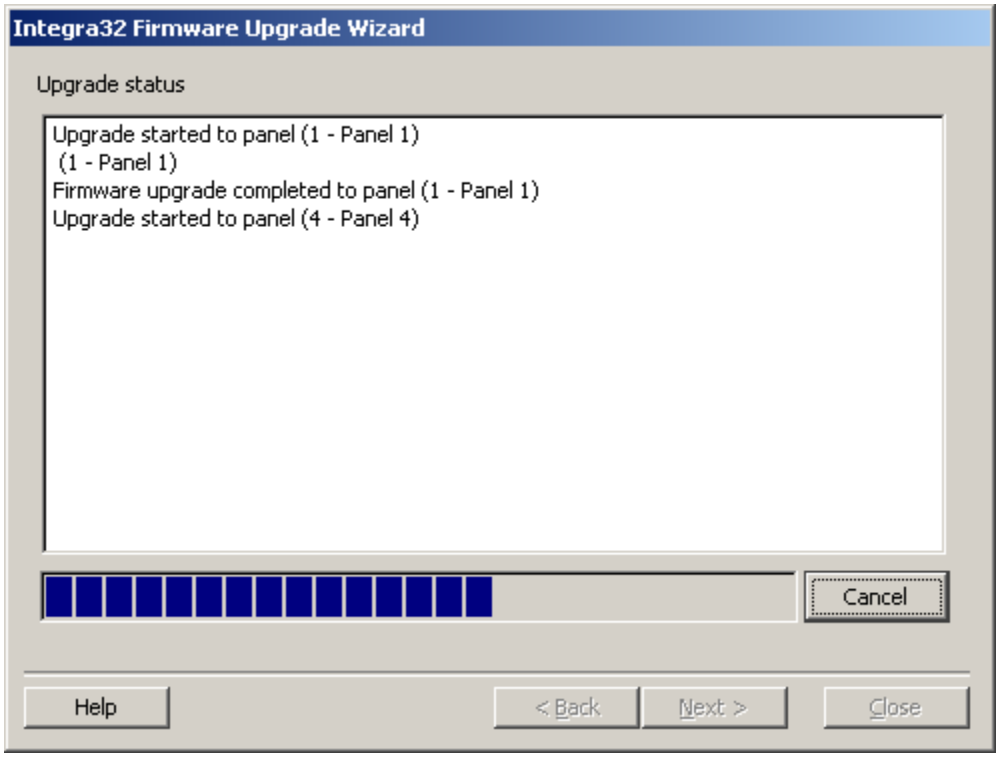


Click ‘Next’ after the appropriate file has been selected.



Next select which panel(s) should be downloaded to. Then click ‘Next’. You don’t have to select all the panels at this time. After upgrading you can come back to this screen.

Clicking ‘Start’ will begin the download.



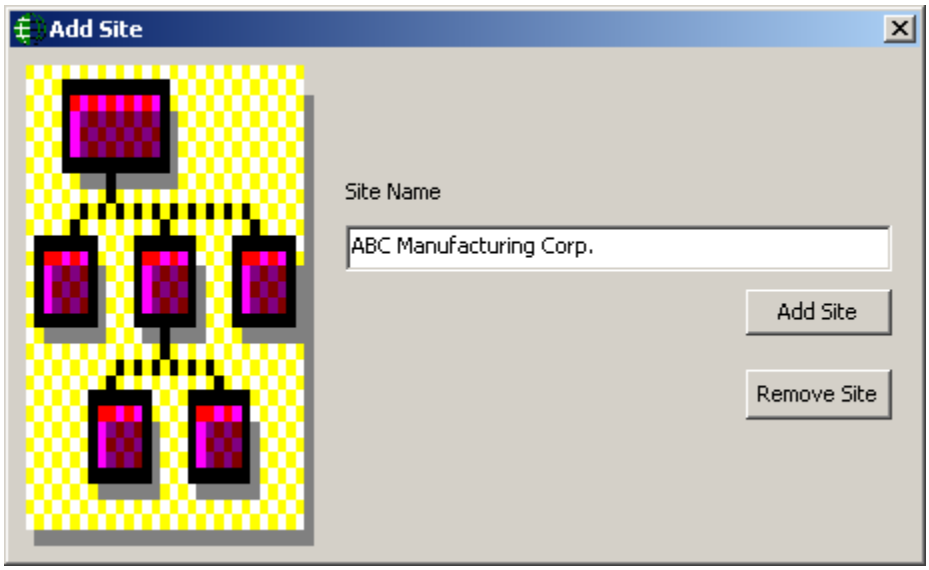
A progress bar and messages will keep informed during the proceedings.

There will be a ‘completed’ message after each panel download. You can go back to select other panels or close if you are finished downloading.

Integra32™ Security System

There are two ways to start the Integra32™ system. You can either double click the icon that was created when the system was installed, or you can click on ‘*Integra32™ Security System*’ in program groups. Both methods will start Integra32™ system.

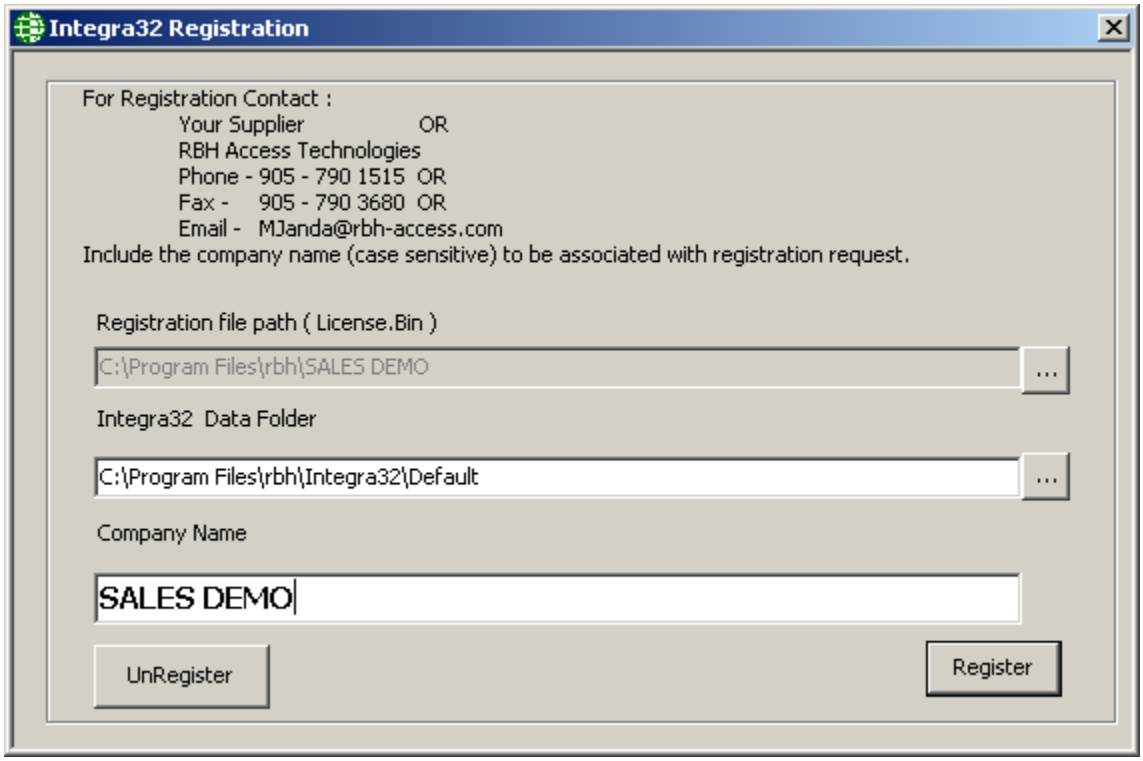
Integra32™ Site Configuration



Type in the name of the site and either click *Add Site* or *Remove Site*. Sites added will be selectable on the server pull-down list while logging-on. Each site will have its own database and maintains its own backup (you must be logged-on to the site at the appropriate time for the auto backup for that site to run).

Integra32™ Registration

The software must be registered in order to enable the Badging software, the Card Import Utility, the Finger Print Reader, the DVR software, and/or the Visitor Management System. None of these features will be accessible or even visible if the license hasn't been registered. Only the feature ordered will be included on a license.



To register the software input the following three pieces of information:

1. Browse for and enter the path to the folder holding the license file (license.bin).
2. Browse for and entry the path to the site folder to be registered. (Each site is registered separately if you have multiple sites.)
3. Enter you company (or site) name.

   Then click *Register*.

Glossary

Many of the words or terms in this guide have more common definitions than used in industry. In this guide, we've used them specifically in the context of security access control. For this reason, the following glossary of terms defines these terms as used in this guide.

Access Point	A point of entry or exit, for an area whose access is controlled and monitored by Integra32™. (*E.g. a door, parking gates*.)
Antipassback (APB)	An Access Control feature designed to prevent improper usage of a valid card.
Ethernet	A widely used LAN developed by Xerox, Digital, and Intel. Ethernet networks connect up to 1,024 nodes at 10 megabits per second over twisted pair, coax, and optical fiber.
Holiday	Any days in which the regular weekly Integra32™ time group schedules are not appropriate. Statutory holidays and summer shut down periods are two examples. In Integra32™, *Holidays* may be assigned special irregular time group schedules that override the regular time group schedule for that day.
Input	Any field apparatus that provides information to an Integra32™ system with respect to conditions or status of a monitored component. Examples include door contacts, thermometers etc.
Operator	Any individual authorized to log-on to the Integra32™ system for purposes of data-entry or monitoring.
Output	Any field apparatus that receives commands from an Integra32™ system and executes the action specified in the command. (Examples include door locks, and lights.)
PIN	Personal Identification Number.
RTE	Request to exit.
TAPI	Telephony Application Programming Interface. TAPI is a Microsoft® Windows set of functions that allows programming of telephone line-based devices in a device-independent manner, giving personal telephony to users.
TCP/IP	Transfer Control Protocol/Internet Protocol. TCP/IP is the protocol that networks use to communicate with each other on the Internet.
Time Group	A *Time Group* (*e.g., Business Hours*) is a pre-defined time slot/day combination that may be assigned to schedules, thereby governing how the Integra32™ system operates from day to day.

License & Warranty

Notice 1.01

This Software is licensed (**not sold**). It is licensed to sublicenses, including end-users, without either express or implied warranties of any kind on an "as is" basis. RBH Access Technologies Inc. makes no express or implied warranties to sublicenses, including end-users, with regard to this software, including merchantability, fitness for any purpose or non-infringement of patents, copyrights, or any other proprietary rights of others. RBH Access Technologies Inc. shall not have any liability or responsibility to sublicenses, including end-users for damages of any kind, including special, indirect or consequential damages arising out of or resulting from any program, services or materials made available hereunder or the or the modification thereof.

Notice 1.02

RBH Access Technologies Inc. makes no claim or warranty with respect to the fitness of any product or software for a specific application and assumes no responsibility for installation. This warranty is in lieu of all other warranties expressed or implied. No representative or agent of RBH Access Technologies Inc. may make any other claims to the fitness of any product for any application.

Index

A

About This Guide 1
Access Levels 82
Access Point Activity 69, 119
Access Points 59
  Advanced 67
  Alarms 64
  CCTV 65
  Links 63
  Modes 60
  Time-Outs 62
Access Points Commands 14
Acknowledge 26
Acknowledge/Unacknowledge/Clear 24
Action Messages 25
Activate Card When Visitor Checks In 114
Alarm Details 24
Alarm Screen 10, 24
Alarm sounds 114
Alarms Toolbar Button 8
Antipassback 67
AP Activity Toolbar Button 8
Area and Cardholder Commands 21
Areas 33
Arm Keypad 23
Auto void cards 114
Auto-Backup 124
Auto-Relock 60

B

Backup 123
Badge Options 115
Badge Template Designer 130

C

Card + PIN Schedule 62
Card Custom Fields 132
Card Format 42
Card Import Utility 5, 133
Cardholders 84
  Cards 90
  More Fields Tab 96
  Options 91
  Photo Tab 94
  Profile Tab 93
  Type 91
Cardholders Toolbar Button 8
Check In 99
Check Out 22, 99
Clear 26
Clear Log 19
Command Bar 3
Command Type 13
Conventions in this guide 1
Copyright ii

D

Data Restore 145
Database Maintenance 145
Database Reports 110
Database Screen 9
Deactivation Date 91
Deduct Usage 60
Disable Forced Entry 60
Disarm Keypad 23
Door Held Open 62
Download 19, 20
DVR Toolbar Button 8

E

Elevators 79
eMail Configuration 120
Event Log Screen 11
Exit 4
Extended Unlock Time 62, 92

F

F Print 85, 88
Facility Code Mode 15, 61
File 4
Finger Print 127
Firmware Upgrade 145
First Person Delay 61
Floor Groups 81
Floors 22
Font 117

G

Getting to Know Integra32 3
Global Antipassback 67
Global Links 122
Glossary 150
Group Cards 114

H

Handicap 92
Help 7
Help Toolbar Button 9
High Security 61
High Security Privilege 92
History Reports 105
Holidays 30

How to Execute a Command 13

I

Ignore Antipassback 91
Import Utility 133
Inhibit ID 61
Input Points Commands 16
Input Properties 70
Inputs
  Alarms 74
  CCTV 71
  Details 70
  Links 73
Integra32 Database 27
Integra32 Server Client Network Setup 2
Integra32™ Database Maintenance 145
Integra32™ Registration 148
Integra32™ Security System 147
Integra32™ Site Configuration 148
Interlock 15
Introducing Integra32 2
IRC2000 Properties 41

K

Keypad Commands 23

L

License & Warranty 151
Link Execute Privilege 91, 92
Links 5
Local Antipassback 67
Log In & Out (Ctrl+L) 4
Login/Logout Toolbar Button 8

M

Magnetic Encoder Setup 116
Menu Options 4
Messages 34
Monitor Screen 12
Multi Cards 85, 86

N

Networks 35
  Advanced 40
  Comms 36
    Direct Connect 36
    Ethernet Connect 39
    Modem Connect 37
  General 35

O

Options 5
Out Reader 68
Output Points Commands 17
Output Properties 75
Outputs
  CCTV 76
  Details 75
  Links 78

P

Panels 41
  Alarms 44
  Code Reader Links 44
  Dial-Out 45
  Reader Options 42
  Site Codes 43
Panels Commands 18
PC Decision Required 61
PC100 48
Permanent Command 13
Preview Reports 106
Print Area Report on Input 114
Program Groups 144
Programming 27
Properties
  Notes Tab 95

Q

Query Finger Print Reader 129

R

rbh.ini 7
Receipt 99
Registration 148
Repeat Ignore Time 63
Reports 6, 105
Reset Area 21
Restore Backup 125
RTE Bypass DC 61
Run Backup Now 123

S

Schedules 31
Semi-Permanent Command 13
Set Area 21
Set Date/Time 19
Site Configuration 148
Status Screen 10
System Messages 118
System Options 113
System Status 12
System Status Toolbar Button 8

T

Time Zone Difference 40
Time Zones 31
Timed Antipassback 63

Timed Command 13
Toolbar Buttons 8
Tools 5, 123
Track Visitor 103, 104

U

Unacknowledge 26
Unlock Privilege 92
Unlock Schedule 62
URC2000 Properties 41
URC2000 with ELV 46
Usage Count 91
User Fields - Visitors 121
User Options 114
Users 27

V

Version 19, 20
Visitor Assets 102
Visitor Manager 97
Visitor Reports 112
Visitor Tracking 103, 104
Visitors' Status 22
Visitors Toolbar Button 8
VM Configuration 120
Void Cards 126

Reader Comments